Anti-Money Laundering Procedures 10.00

Introduction

In accordance with the requirements of Title III of the *USA Patriot Act of 2001* and *FINRA Rule 3310*, each member shall develop and implement a written anti-money laundering program reasonably designed to achieve and monitor the member's compliance with the requirements of the Bank Secrecy Act (31 U.S.C. 5311, *et seq*.), and the implementing regulations promulgated thereunder by the Department of the Treasury. Each member's anti-money laundering program must be approved, in writing, by a member of senior management. The anti-money laundering programs required by this Rule shall, at a minimum,

(a) Establish and implement policies and procedures that can be reasonably expected to detect and cause the reporting of transactions required under 31 U.S.C. 5318(g) and the implementing regulations thereunder;

(b) Establish and implement policies, procedures, and internal controls reasonably designed to achieve compliance with the Bank Secrecy Act and the implementing regulations thereunder;

(c) Provide for annual (on a calendar-year basis) independent testing for compliance to be conducted by member personnel or by a qualified outside party, unless the member does not execute transactions for customers or otherwise hold customer accounts or act as an introducing broker with respect to customer accounts (e.g., engages solely in proprietary trading or conducts business only with other broker-dealers), in which case such "independent testing" is required every two years (on a calendar-year basis);

(d) Designate and identify to FINRA (by name, title, mailing address, e-mail address, telephone number, and facsimile number) an individual or individuals responsible for implementing and monitoring the day-to-day operations and internal controls of the program (such individual or individuals must be an associated person of the member) and provide prompt notification to FINRA regarding any change in such designation(s); and

(e) Provide ongoing training for appropriate personnel.

Therefore, the Firm has adopted and implemented certain policies and procedures against money laundering and any direct or indirect activity which may facilitate the act of money laundering or the funding of terrorist or other criminal activity. The Firm strongly believes it is the responsibility of all members of management as well as every employee to protect the Firm from any potential exploitation by money laundering activities which may jeopardize the Firm's overall compliance with relevant federal, state and SRO rules and regulations. The Firm will comply with its obligation to monitor new rules under Section 311 of the USA Patriot Act. In order to fulfill its obligation, the Firm's designated AMLCO may review updated information by clicking on the following link (http://www.fincen.gov/statutes_regs/patriot/section311.html) or access this information through other available sources.

The following procedures are designed to combat money laundering activity, to include those rules and regulations requiring the mandatory reporting of certain transactions involving currency, monetary instruments and suspicious activity.

10.01 Designations/Responsibilities for Anti-Money Laundering Procedures

The Firm shall assign certain responsibilities to a designated compliance officer, unit, group or committee for the proper execution of anti-money laundering related policies and procedures. The designated person(s) shall be the Firm's central point of contact for any/all communications with regulatory agencies regarding the Firm's anti-money laundering program.

Additionally, in accordance with *FINRA NTM 02-78*, the Firm shall designate and identify to FINRA (by name, title, mailing address, e-mail address, telephone number, and facsimile number) any and/or all individuals responsible for implementing and monitoring the day-to-day operations and internal controls of the Firm's anti-money laundering policies and procedures and provide prompt notification to FINRA regarding any change in such designation(s).

Designated Compliance Officer, Unit, Group, Dept. or Committee

Note: Please see the Firm's List of Supervisory Personnel for further details on the designated AML Contact Person who is responsible for all relevant AML compliance monitoring and supervision.

Anti-Money Laundering Contacts

With the recent designation of the Firm's compliance officer for anti-money laundering policies and procedures, all firm personnel shall be provided with a "point-of-contact" sheet detailing primary and alternate designated contact persons along with corresponding telephone numbers for any questions or concerns on anti-money laundering issues, policies and procedures.

Approval of AML Program by Senior Management

The Firm has implemented an internal policy that requires a designated member of senior management to review and approve the AML policies and procedures ("Program").

Note: Please see the Firm's Approval of AML Program by Senior Management for further details.

Implementation Strategy

The Firms designated primary and alternate AML Compliance Contacts are listed on FINRA's Contact System (FCS).

10.02 Monitoring of Account Activities

One of the main objectives for the continuous monitoring of customer account activities is the potential detection and prevention of suspicious and unusual transactions relating to money laundering activities. Based on the Firm's size, scope and product focus, there are several differing methods as to the proper monitoring of customer account activities. For the monitoring of such activities, the Firm may choose to implement internal manual methods for monitoring or may use some form of external automated monitoring system specific to the firm.

In the design and implementation of the Firm's monitoring efforts, the following areas shall be closely monitored for potential money laundering activities:

Wire Transfer Activity

All broker/dealer firms that accept wire transfers shall set certain parameters for monitoring such transactional activities. Such parameters for wire transfer activities should include specific dollar amounts, volume thresholds and wire transfers directed toward certain geographic destinations identified as "high risk;"

Deposits

All broker/dealer firms that accept cash (i.e. currency) at the deposit stage shall set certain parameters for monitoring such transactional activities. For example, if a firm has established certain limitations on the amount of each cash deposit that can be received, the monitoring should review for exceptions to such limitations. However, if no current and established limitations on deposit amounts exist, at a minimum, a firm should monitor deposits aggregating in excess of $10,000.

Monetary Instruments

In the event that broker/dealer firms accept cash or cash equivalents, including cashier's checks, money orders and traveler's checks, certain procedures should be implemented to monitor for the "structuring" of such deposits. ►►

Note: The term "Structuring" is the process of attempting to spread deposits of currency or other cash equivalents on a single day, over a number of days or in a number of accounts so as to avoid suspicion or mandatory filing requirements for deposits over certain specific thresholds.

Implementation Strategy

The Firm is classified as an "introducing" broker/dealer and does not accept customer funds or securities. Therefore, the Firm shall adopt and rely on certain monitoring methods to be used by its designated clearing firm to include reporting systems and/or activity/exception-based reporting systems in the continuous review of customer account and transactional activity involving wire transfers, cash deposits and other monetary instruments. On a periodic basis, the AML contact person will review incoming deposits to and outgoing withdrawals from the clearing firm and evidence such review on an ongoing basis.

10.03 Reporting of Suspicious Activities (Money Laundering "Red Flags")

Under Treasury's SAR rule, a broker-dealer must report a transaction to the Financial Crimes Enforcement Network (FinCEN) if it is conducted or attempted by, at or through a broker-dealer, it involves or aggregates funds or other assets of at least $5,000, and the broker-dealer knows, suspects or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part):

- involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location or control of such funds or assets) as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;
- is designed, whether through structuring or other means, to evade any regulations promulgated under the BSA;
- has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the broker-dealer knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or
- involves use of the broker-dealer to facilitate criminal activity

Broker-dealers must report the suspicious activity by completing a SAR and filing it in accordance with the requirements of Treasury's SAR rule. Broker-dealers must maintain a copy of any SAR filed and supporting documentation for a period of five years from the date of filing the SAR. FinCEN has provided guidance to the industry advising that if the activity that was the subject of a SAR filing continues, firms should review any continuing activity at least every 90 days to consider whether a continuing activity SAR filing is warranted, with the filing deadline being 120 days after the date of the previously related SAR filing.

In situations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, broker-dealers must immediately notify by telephone an appropriate law enforcement authority in addition to filing timely a SAR. The firm may call FinCEN's Hotline at (866) 556-3974.

Money Laundering Red Flags

FINRA published a list of "money laundering red flags" in Notice to Members 02-21 (NTM 02-21). Since NTM 02-21 was published, guidance detailing additional red flags that may be applicable to the securities industry have been published by a number of U.S. government agencies and international organizations. The following is a list of additional money laundering red flags for firms to consider incorporating into their AML programs, as may be appropriate in implementing a risk-based approach to BSA/AML compliance:

Potential Red Flags in Customer Due Diligence and Interactions With Customers

1. The customer provides the firm with unusual or suspicious identification documents that cannot be readily verified or are inconsistent with other statements or documents that the customer has provided. Or, the customer provides information that is inconsistent with other available information about the customer. This indicator may apply to account openings and to interaction subsequent to account opening.

2. The customer is reluctant or refuses to provide the firm with complete customer due diligence information as required by the firm's procedures, which may include information regarding the nature and purpose of the customer's business, prior financial relationships, anticipated account activity, business location and, if applicable, the entity's officers and directors.

3. The customer refuses to identify a legitimate source of funds or information is false, misleading or substantially incorrect.

4. The customer is domiciled in, doing business in or regularly transacting with counterparties in a jurisdiction that is known as a bank secrecy haven, tax shelter, high-risk geographic location (e.g., known as a narcotics producing jurisdiction, known to have ineffective AML/Combating the Financing of Terrorism systems) or conflict zone, including those with an established threat of terrorism.

5. The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.

6. The customer has no discernable reason for using the firm's service or the firm's location (e.g., the customer lacks roots to the local community or has gone out of his or her way to use the firm).

7. The customer has been rejected or has had its relationship terminated as a customer by other financial services firms.

8. The customer's legal or mailing address is associated with multiple other accounts or businesses that do not appear related.

9. The customer appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.

10. The customer is a trust, shell company or private investment company that is reluctant to provide information on controlling parties and underlying beneficiaries.

11. The customer is publicly known or known to the firm to have criminal, civil or regulatory proceedings against him or her for crime, corruption or misuse of public funds, or is known to associate with such persons. Sources for this information could include news items, the Internet or commercial database searches.

12. The customer's background is questionable or differs from expectations based on business activities.

13. The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, with no apparent business or other purpose.

14. An account is opened by a politically exposed person (PEP), particularly in conjunction with one or more additional risk factors, such as the account being opened by a shell company beneficially owned or controlled by the PEP, the PEP is from a country which has been identified by FATF as having strategic AML regime deficiencies, or the PEP is from a country known to have a high level of corruption.

15. An account is opened by a non-profit organization that provides services in geographic locations known to be at higher risk for being an active terrorist threat.

16. An account is opened in the name of a legal entity that is involved in the activities of an association, organization or foundation whose aims are related to the claims or demands of a known terrorist entity.

17. An account is opened for a purported stock loan company, which may hold the restricted securities of corporate insiders who have pledged the securities as collateral for, and then defaulted on, purported loans, after which the securities are sold on an unregistered basis.

18. An account is opened in the name of a foreign financial institution, such as an offshore bank or broker-dealer, that sells shares of stock on an unregistered basis on behalf of customers.

19. An account is opened for a foreign financial institution that is affiliated with a U.S. broker-dealer, bypassing its U.S. affiliate, for no apparent business purpose. An apparent business purpose could include access to products or services the U.S. affiliate does not provide.

Potential Red Flags in Deposits of Securities

1. A customer opens a new account and deposits physical certificates, or delivers in shares electronically, representing a large block of thinly traded or low-priced securities.

2. A customer has a pattern of depositing physical share certificates, or a pattern of delivering in shares electronically, immediately selling the shares and then wiring, or otherwise transferring out the proceeds of the sale(s).

3. A customer deposits into an account physical share certificates or electronically deposits or transfers shares that:

    - were recently issued or represent a large percentage of the float for the security;

- reference a company or customer name that has been changed or that does not match the name on the account;
- were issued by a shell company;
- were issued by a company that has no apparent business, revenues or products;
- were issued by a company whose SEC filings are not current, are incomplete, or nonexistent;
- were issued by a company that has been through several recent name changes or business combinations or recapitalizations;
- were issued by a company that has been the subject of a prior trading suspension; or
- were issued by a company whose officers or insiders have a history of regulatory or criminal violations, or are associated with multiple low-priced stock issuers.

4. The lack of a restrictive legend on deposited shares seems inconsistent with the date the customer acquired the securities, the nature of the transaction in which the securities were acquired, the history of the stock or the volume of shares trading.

5. A customer with limited or no other assets at the firm receives an electronic transfer or journal transfer of large amounts of low-priced, non-exchange-listed securities.

6. The customer's explanation or documents purporting to evidence how the customer acquired the shares does not make sense or changes upon questioning by the firm or other parties. Such documents could include questionable legal opinions or securities purchase agreements.

7. The customer deposits physical securities or delivers in shares electronically, and within a short time-frame, requests to journal the shares into multiple accounts that do not appear to be related, or to sell or otherwise transfer ownership of the shares.

8. Seemingly unrelated clients open accounts on or at about the same time, deposit the same low-priced security and subsequently liquidate the security in a manner that suggests coordination.

Potential Red Flags in Securities Trading

1. The customer, for no apparent reason or in conjunction with other "red flags," engages in transactions involving certain types of securities, such as penny stocks, Regulation "S" stocks and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)

2. There is a sudden spike in investor demand for, coupled with a rising price in, a thinly traded or low-priced security.

3. The customer's activity represents a significant proportion of the daily trading volume in a thinly traded or low-priced security.

4. A customer buys and sells securities with no discernable purpose or circumstances that appear unusual.

5. Individuals known throughout the industry to be stock promoters sell securities through the broker-dealer.

6. A customer accumulates stock in small increments throughout the trading day to increase price.

7. A customer engages in pre-arranged or other non-competitive securities trading, including wash or cross trades, with no apparent business purpose.

8. A customer attempts to influence the closing price of a stock by executing purchase or sale orders at or near the close of the market.

9. A customer engages in transactions suspected to be associated with cyber breaches of customer accounts, including potentially unauthorized disbursements of funds or trades.

10. A customer engages in a frequent pattern of placing orders on one side of the market, usually inside the existing National Best Bid or Offer (NBBO), followed by the customer entering orders on the other side of the market that execute against other market participants that joined the market at the improved NBBO (activity indicative of “spoofing”).

11. A customer engages in a frequent pattern of placing multiple limit orders on one side of the market at various price levels, followed by the customer entering orders on the opposite side of the market that are executed and the customer cancelling the original limit orders (activity indicative of “layering”).

12. Two or more unrelated customer accounts at the firm trade an illiquid or low-priced security suddenly and simultaneously.

13. The customer makes a large purchase or sale of a security, or option on a security, shortly before news or a significant announcement is issued that affects the price of the security.

14. The customer is known to have friends or family who work at or for the securities issuer, which may be a red flag for potential insider trading or unlawful sales of unregistered securities.

15. The customer’s purchase of a security does not correspond to the customer’s investment profile or history of transactions (e.g., the customer may never have invested in equity securities or may have never invested in a given industry, but does so at an opportune time) and there is no reasonable explanation for the change.

16. The account is using a master/sub structure, which enables trading anonymity with respect to the sub-accounts’ activity, and engages in trading activity that raises red flags, such as the liquidation of microcap issuers or potentially manipulative trading activity.

17. The firm receives regulatory inquiries or grand jury or other subpoenas concerning the firm’s customers’ trading.

18. The customer engages in a pattern of transactions in securities indicating the customer is using securities to engage in currency conversion. For example, the customer delivers in and subsequently liquidates American Depository Receipts (ADRs) or dual currency bonds for U.S. dollar proceeds, where the securities were originally purchased in a different currency.

19. The customer engages in mirror trades or transactions involving securities used for currency conversions, potentially through the use of offsetting trades.

20. The customer appears to buy or sell securities based on advanced knowledge of pending customer orders.

Potential Red Flags in Money Movements

1. The customer attempts or makes frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the firm's policies and procedures relating to the deposit of cash and cash equivalents.

2. The customer "structures" deposits, withdrawals or purchases of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements,and may state directly that they are trying to avoid triggering a reporting obligation or to evade taxing authorities.

3. The customer seemingly breaks funds transfers into smaller transfers to avoid raising attention to a larger funds transfer. The smaller funds transfers do not appear to be based on payroll cycles, retirement needs, or other legitimate regular deposit and withdrawal strategies.

4. The customer's account shows numerous currency, money order (particularly sequentially numbered money orders) or cashier's check transactions aggregating to significant sums without any apparent business or lawful purpose.

5. The customer frequently changes bank account details or information for redemption proceeds, in particular when followed by redemption requests.

6. The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.

7. Wire transfers are made in small amounts in an apparent effort to avoid triggering identification or reporting requirements.

8. Incoming payments are made by third-party checks or checks with multiple endorsements.

9. Outgoing checks to third parties coincide with, or are close in time to, incoming checks from other third parties.

10. Payments are made by third party check or money transfer from a source that has no apparent connection to the customer.

11. Wire transfers are made to or from financial secrecy havens, tax havens, high risk geographic locations or conflict zones, including those with an established presence of terrorism.

12. Wire transfers originate from jurisdictions that have been highlighted in relation to black market peso exchange activities.

13. The customer engages in transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (e.g., countries designated by national authorities, such as FATF, as non-cooperative countries and territories).

14. The parties to the transaction (e.g., originator or beneficiary) are from countries that are known to support terrorist activities and organizations.

15. Wire transfers or payments are made to or from unrelated third parties (foreign or domestic), or where the name or account number of the beneficiary or remitter has not been supplied.

16. There is wire transfer activity that is unexplained, repetitive, unusually large, shows unusual patterns or has no apparent business purpose.

17. The securities account is used for payments or outgoing wire transfers with little or no securities activities (i.e., account appears to be used as a depository account or a conduit for transfers, which may be purported to be for business operating needs).

18. Funds are transferred to financial or depository institutions other than those from which the funds were initially received, specifically when different countries are involved.

19. The customer engages in excessive journal entries of funds between related or unrelated accounts without any apparent business purpose.

20. The customer uses a personal/individual account for business purposes or vice versa.

21. A foreign import business with U.S. accounts receives payments from outside the area of its customer base.

22. There are frequent transactions involving round or whole dollar amounts purported to involve payments for goods or services.

23. Upon request, a customer is unable or unwilling to produce appropriate documentation (e.g., invoices) to support a transaction, or documentation appears doctored or fake (e.g., documents contain significant discrepancies between the descriptions on the transport document or bill of lading, the invoice, or other documents such as the certificate of origin or packing list).

24. The customer requests that certain payments be routed through nostro[14] or correspondent accounts held by the financial intermediary instead of its own accounts, for no apparent business purpose.

25. Funds are transferred into an account and are subsequently transferred out of the account in the same or nearly the same amounts, especially when the origin and destination locations are high-risk jurisdictions.

26. A dormant account suddenly becomes active without a plausible explanation (e.g., large deposits that are suddenly wired out).

27. Nonprofit or charitable organizations engage in financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.

28. There is unusually frequent domestic and international automated teller machine (ATM) activity.

29. A person customarily uses the ATM to make several deposits into a brokerage account below a specified BSA/AML reporting threshold.

30. Many small, incoming wire transfers or deposits are made using checks and money orders that are almost immediately withdrawn or wired out in a manner inconsistent with the customer's business or history; the checks or money orders may reference in a memo section "investment" or "for purchase of stock." This may be an indicator of a Ponzi scheme or potential funneling activity.

31. Wire transfer activity, when viewed over a period of time, reveals suspicious or unusual patterns, which could include round dollar, repetitive transactions or circuitous money movements.

Potential Red Flags in Insurance Products

1. The customer cancels an insurance contract and directs that the funds be sent to a third party.

2. The customer deposits an insurance annuity check from a cancelled policy and immediately requests a withdrawal or transfer of funds.

3. The customer cancels an annuity product within the free-look period. This could be a red flag if accompanied with suspicious indicators, such as purchasing the annuity with several sequentially numbered money orders or having a history of cancelling annuity products during the free-look period.

4. The customer opens and closes accounts with one insurance company, then reopens a new account shortly thereafter with the same insurance company, each time with new ownership information.

5. The customer purchases an insurance product with no concern for the investment objective or performance.

Potential Red Flags of Fraud Involving Low-Priced Securities

The following non-exhaustive list of issuer, third-party and/or customer activities may be red flags of fraud involving low-priced securities:

Issuers

1. abrupt or frequent changes of issuer name, ticker symbol or business model, or abrupt expansion of an existing business model, often to benefit from the latest trend such as COVID-19 cures, test kits or prevention-related products (including instances in which the issuer has previously engaged in a business involved with other trends such as e-cigarettes, cannabis or cryptocurrency);
2. currently or previously a shell company;

3. engaging in recapitalization or reorganization activities (*e.g.*, a reverse or forward stock split in conjunction with a reverse merger) that appear to concentrate the shares into the hands of a small number of shareholders, who may be acting in coordination;

4. hiring executive or control persons or service providers—such as attorneys, auditors, transfer agents, consultants and promoters—who have a history of regulatory or criminal violations, or are associated with multiple low-priced stock issuers;

5. not providing current and adequate publicly available financial information in SEC filings or voluntary disclosures on an inter-dealer quotation system;

6. making claims about projected scale and revenue targets that are not supported by the issuer's experience, assets or financial condition (*e.g.*, an issuer that develops cannabinoid-based products announces that it could earn millions in revenue from manufacturing and shipping COVID-19 home test kits);

7. making unsupported claims regarding partnerships, joint ventures or financing agreements with private entities (*e.g.*, an issuer promotes a press release touting the financial benefits of a new business partnership with a company whose financial condition cannot be independently verified);

8. conducting increased social media, press release or related investor outreach campaigns after a period of apparent dormancy, particularly if the information is not confirmed on the issuer's website or in financial statements and disclosures filed with the SEC or on an inter-dealer quotation system, and often related to the latest trend; or

9. lacking verifiable evidence of the issuer's business activities, such as limited or no operational website, social media accounts, references to issuer on employment websites or other independent reporting on the issuer's business activities.

Third-Party Promotional Activities

1. hyping and promoting issuers (or their products or services), especially where the information cannot be reliably confirmed;

2. promotional investor email alerts, banner advertisements, dedicated promotional websites or seemingly independent news or research coverage, which prominently feature or advertise the issuer's new potential business prospects that (1) may be related to the latest trend (*e.g.*, winning a large contract or developing a new product or service), (2) may also present recent or projected investment returns, and (3) cannot be reliably confirmed;

3. generating a spike in social media promotions (*e.g.*, on Twitter, Instagram or Facebook), and activity on investor chat rooms or message boards; or

4. conducting unsolicited phone calls or sending text alerts to tout specific stocks to garner interest from registered representatives and investors.

Firm Customers

1. customers that deposit large blocks of thinly traded low-priced securities, whether the securities are marked with a restrictive legend or not, particularly of issuers that recently changed business models to take advantage of the latest trend;

2. customers that engage in transactions that are consistent with an intent to affect the price of a low-priced stock, such as small purchases executed on behalf of a customer who owns a very large amount of the same low-priced stock, and do not have a legitimate investment rationale for the transactions;

3. customers that engage in a pattern of purchasing a low-priced security right before market close (which may be indicative of an attempt to mark the close);

4. customers or other parties that request the firm file a FINRA Form 211 to initiate or resume quotations for an issuer that recently changed business models—often to take advantage of the latest trend—or was recently subject to a trading suspension;

5. current officers, former officers, significant shareholders or family members of these individuals, who trade low-priced securities prior to a corporate announcement or stock promotion campaign;

6. one or more customers suddenly trading the securities of a thinly traded issuer—often one that makes claims related to the latest trend—on opposite sides of the market, potentially leading to manipulative trading;

7. customers, particularly specified adults, who are being solicited to purchase low-priced securities where (1) the customer has not invested in low-priced securities previously; (2) the purchase is outside the customer's investment or risk profile; or (3) the low-priced security constitutes a large concentration of the customer's investments;

8. multiple new customers opening accounts (particularly if they reside overseas and communicate with the firm only through electronic means) who either deposit shares of the same issuer or were introduced by the same individual to the firm; or

9. customers, including financial institutions, that route high volume or frequent sell orders (with no buys) for low-priced securities to the firm for execution, including customers who maintain an execution-only relationship with the firm, or use omnibus or Delivery versus Payment/Receive versus Payment (DVP/RVP) accounts for such transactions. (Ref. Regulatory Notice 21-03; February 10, 2021)

Implementation Strategy

To the extent reasonable and applicable, the Firm will consider implementing one or more of the following supervisory controls related to low-priced securities.

Supervision of Associated Persons

- monitoring registered representatives' customers' investments in low-priced securities that are marked "unsolicited" to determine if the trades were in fact solicited;
- monitoring registered representatives' solicitations to customers to trade low-priced securities for compliance with FINRA rules and applicable laws;
- monitoring the proprietary and customer accounts of registered representatives who primarily trade in low-priced securities; and
- enhancing supervision of registered representatives who maintain direct or indirect outside business activities associated with companies with low-priced shares or trade in low-priced securities in their outside brokerage accounts.

Account and Share Acceptance

- establishing risk-based criteria to determine the characteristics of securities (e.g., exchange-listed and SEC reporting companies) investors may hold in their accounts or in which they may initiate transactions on the firm's platform;
- establishing controls to identify situations where customers open new accounts and deposit or transfer large blocks of low-priced securities, including in omnibus or DVP/RVP accounts;
- promptly reviewing deposits of physical certificates and electronic transfers of low-priced securities prior to acceptance to identify low-priced securities that are marked as restricted, as well as low-priced securities that are not marked restricted where the restrictive legend may have been inappropriately lifted;
- implementing risk-based acceptance policies regarding physical and electronic deposits of low-priced securities that incorporate factors such as whether the issuer is exchange-listed, the markets or exchanges on which it trades, any compliance flags that exchanges and over-the-counter markets provide regarding the issuer;
- requiring compliance or AML department approval of exceptions to firm policies on the deposit and trading of low-priced securities by customers; and
- obtaining information regarding the customer's occupation or business and establishing risk-based criteria to request additional information, such as whether the customer is employed by a company that trades on the public markets and whether the customer intends to deposit or trade low-priced securities.

Account Monitoring

- monitoring customer accounts for shifts in investment strategy away from listed equities towards unlisted low-priced securities, especially if this is inconsistent with the customer's stated or historic risk tolerance;
- monitoring accounts held by specified adults and seniors for unusual purchases, or high concentrations, of low-priced securities and, where appropriate, contacting customers to determine if these decisions were the result of solicitation or influence by a third party;
- monitoring customer accounts, including omnibus or DVP/RVP accounts, that are liquidating low-priced securities to address risks relating to the firm being engaged in, among other things, an unregistered securities offering;
- establishing risk-based criteria to determine the circumstances under which a firm would consider placing restrictions on or closing an account;
- monitoring for groups of related accounts trading in the same low-priced security at the same time; and
- reviewing for indications of stock promotion activity in connection with share acceptance and account monitoring reviews.

Other Controls

- conducting education and outreach—which could include providing risk alerts at the time of order entry—to customers, especially specified adults, to inform them about the risks of investing in low-priced securities;
- identifying and, if necessary, prohibiting customers from opening new accounts with, or depositing in existing accounts, restricted shares of low-priced listed or low-priced OTC securities; and
- increasing training and coordination between risk, compliance and operational personnel to ensure frontline staff are aware of red flags associated with potential fraud involving low-priced securities and schemes to unlawfully distribute unregistered securities and know how to report their concerns. (Ref. Regulatory Notice 21-03; February 10, 2021)

Other Potential Red Flags

1. The customer is reluctant to provide information needed to file reports to proceed with the transaction.

2. The customer exhibits unusual concern with the firm's compliance with government reporting requirements and the firm's AML policies.

3. The customer tries to persuade an employee not to file required reports or not to maintain the required records.

4. Notifications received from the broker-dealer's clearing firm that the clearing firm had identified potentially suspicious activity in customer accounts. Such notifications can take the form of alerts or other concern regarding negative news, money movements or activity involving certain securities.

5. Law enforcement has issued subpoenas or freeze letters regarding a customer or account at the securities firm.

6. The customer makes high-value transactions not commensurate with the customer's known income or financial resources.

7. The customer wishes to engage in transactions that lack business sense or an apparent investment strategy or are inconsistent with the customer's stated business strategy.

8. The stated business, occupation or financial resources of the customer are not commensurate with the type or level of activity of the customer.

9. The customer engages in transactions that show the customer is acting on behalf of third parties with no apparent business or lawful purpose.

10. The customer engages in transactions that show a sudden change inconsistent with normal activities of the customer.

11. Securities transactions are unwound before maturity, absent volatile market conditions or other logical or apparent reason.

12. The customer does not exhibit a concern with the cost of the transaction or fees (e.g., surrender fees, or higher than necessary commissions).

13. A borrower defaults on a cash-secured loan or any loan that is secured by assets that are readily convertible into currency.

14. There is an unusual use of trust funds in business transactions or other financial activity.

Suspicious Activity Reporting (SAR) Requirements

An effective compliance program includes certain controls and measures to identify and report suspicious transactions in timely manner. Every broker/dealer firm must apply due diligence to be able to make an informed decision about the suspicious nature of a particular transaction and whether to file a Suspicious Activity Report by the Securities and Futures Industry (SAR-SF).

In accordance with *Section 356 of Title III of the Patriot Act* and *NTM 02-47*, the Treasury Department has published a new form, "Suspicious Activity Report by the Securities and Futures Industry" (SAR-SF). While the Treasury's final SAR rule indicated that it was developing a suspicious activity reporting form for broker/dealers entitled "Suspicious Activity Report Brokers or Dealers in Securities" (SAR-BD), the Treasury has indicated that the Form could also be used by futures commission merchants (FCMs) registered with the Commodity Futures Trading Commission (CFTC). Accordingly, the draft Form has been revised from SAR-BD to SAR-SF and several fields have been provided on the Form for use by FCMs.

Therefore, the following terms and condition shall apply for reporting and/or filing of a Suspicious Activity Report by the Securities and Futures Industry (SAR-SF) with the Financial Crimes Enforcement Network (FinCEN):

Dollar Threshold for Reporting

The reporting threshold in FinCEN's SAR rule is $5,000, regardless of the nature of the suspicious transaction reported. Therefore, all broker/dealers are required to report suspicious transactions of at least $5,000.

Reporting Standard

All broker/dealers are required to report any suspicious activity as referenced above if the broker/dealer knows, suspects, or has reason to suspect that a transaction requires reporting under the rule.

Reporting Time Requirements

Each broker/dealer that becomes aware of any suspicious transactions must report such transactions by completing a SAR-SF and filing it within thirty (30) days of discovery. If a broker/dealer is unable to identify a suspect on the date the suspicious transaction is initially detected, the broker/dealer will have an addition thirty (30) calendar days to identify the suspect before filing a SAR-SF, but the suspicious transaction must be

reported within sixty (60) calendar days after the date of the initial detection of the suspicious transaction, whether or not the broker/dealer is able to identify a suspect.

Scope of Reporting

For any transaction aggregating $5,000 or more that involves potential violations of the *Bank Secrecy Act* or other related rules and regulations, there are four (4) categories of reportable transaction:

- Any transaction involving funds derived from illegal activity or intended or conducted to hide or disguise funds or assets derived from illegal activity;
- Any transaction designed, whether through "structuring" or other means, to evade the requirements of the Bank Secrecy Act (BSA);
- Any transaction that appears to serve no business or apparent lawful purpose or the sort of transaction in which the particular customer would normally be expected to engage, and for which the broker/dealer knows of no reasonable explanation after examining the available facts;
- Any transactions involving legally-derived funds that the broker/dealer suspects are being used for a criminal purpose (e.g. transactions that the broker/dealer suspects are designed to fund terrorist activity);

Exceptions from Reporting

Certain exceptions from filing a SAR-SF with the FinCEN shall apply under the following conditions:

- A robbery or burglary committed or attempted of the broker/dealer that is reported to appropriate law enforcement authorities, or for lost, missing, counterfeit, or stolen securities with respect to which the broker/dealer files a report pursuant to the reporting requirements of *17 CFR 240.17f-1*;
- A violation otherwise required to be reported under any of the federal securities laws or rules of an SRO by the broker/dealer or any of its officers, directors, employees, or other registered representatives, other than a violation of *17 CFR 240.17a-8* or *17 CFR 405.4* so long as such violation is appropriately reported to the SEC or an SRO.

Minimum Reporting Requirements

In accordance with the *Bank Secrecy Act, Section 356 of the PATRIOT Act* and other related federal rules and regulations on Money Laundering, the Firm will comply with all relevant reporting requirements specific to the Firm's current needs by filing one or more of the following reports:

FinCEN Suspicious Activity Report (FinCEN Report 111)

Banks and other financial institutions must file a SAR for any suspicious transaction relevant to a possible violation of law or regulation. (*31 CFR 103.18- formerly 31 CFR 103.21*) (*12 CFR 12.11*) ►►

Implementation Strategy

Upon the discovery of any potential suspicious activity as referenced herein and as noted on the Suspicious Activity Report by the Securities and Futures Industry (SAR-SF) in *When To Make A Report*, the designated principal will complete and file a SAR-SF through the BSA E-Filing System.

All completed and filed SAR reports will be maintained at the Firm's main office location in accordance with books and records requirements.

FinCEN Currency Transaction Report (FinCEN Report 112)

A CTR must be filed for each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through or to a financial institution, which involves a transaction in currency of *more than* $10,000. Multiple currency transactions must be treated as a single transaction if the financial institution *has knowledge* that: (a) they are conducted by or on behalf of the same person; (b) they result in cash received or disbursed by the financial institution of more than $10,000. (*31 CFR 103.22*) ►►

Implementation Strategy

For any deposit, withdraw, exchange of currency, or other payment or transfer, by, through or to the Firm totaling more than $10,000, the designated principal shall complete a Currency Transaction Report (CTR) file by the 15th calendar day after the day of the transaction through the BSA E-Filing System.

All completed and filed CTR forms will be maintained at the Firm's main office location in accordance with books and records requirements.

Report of International Transportation of Currency or Monetary Instruments (CMIR) (FinCEN Report 105)

Each person (including a bank) who physically transports, mails or ships, or causes to be physically transported, mailed, shipped or received, currency, traveler's checks, and certain other monetary instruments in an aggregate amount *exceeding* $10,000 into or out of the United States must file a CMIR. (*31 CFR 103.23*) ►►

Implementation Strategy

The Firm does not engage in transporting, mailing or shipping currency, traveler's checks, or other monetary instruments into or out of the United States that exceed $10,000. However, in the event the Firm is required to file a CMIR, all CMIR reports are to be filed through the BSA E-Filing System.

Report of Foreign Bank and Financial Accounts (FinCEN Report 114)

FinCEN Form 114, Report of Foreign Bank and Financial Accounts is used to report a financial interest in or signature authority over a foreign financial account. The FBAR must be received by the Department of the Treasury on or before April 15th of the year immediately following the calendar year being reported. FinCEN will grant filers failing to meet the FBAR annual due date of April 15th an automatic extension to October 15th each year. Accordingly, specific requests for this extension are not required. A United States person that has a financial interest in or signature authority over foreign financial

accounts must file an FBAR if the aggregate value of the foreign financial accounts exceeds $10,000 at any time during the calendar year. ►►

Implementation Strategy

The Firm does not have an interest in, signature power or other authority over, one or more bank, securities, or other financial accounts located in a foreign country. However, in the event the Firm is required to file a FBAR, all FBAR reports are to be filed through the BSA E-Filing System.

Note: The new annual due date for filing Reports of Foreign Bank and Financial Accounts (FBAR) for foreign financial accounts is April 15. This date change was mandated by the Surface Transportation and Veterans Health Care Choice Improvement Act of 2015, Public Law 114-41 (the Act). Specifically, section 2006(b)(11) of the Act changes the FBAR due date to April 15 to coincide with the Federal income tax filing season. The Act also mandates a maximum six-month extension of the filing deadline. To implement the statute with minimal burden to the public and FinCEN, FinCEN will grant filers failing to meet the FBAR annual due date of April 15 an automatic extension to October 15 each year. Accordingly, specific requests for this extension are not required. (Please note: The due date for FBAR filings for foreign financial accounts maintained during calendar year 2016 is April 18, 2017, consistent with the Federal income tax due date.)

FinCEN Designation of Exempt Person (DOEP) (FinCEN Report 110)

The Bank Secrecy Act and its implementing regulations require banks to file currency transaction reports on transactions in currency of more than $10,000. The regulations also permit a bank to exempt certain customers from currency transaction reporting in accordance with 31 CFR 1020.315. Banks are the only type of financial institutions that may exempt customers from CTR filing requirements. The term bank is defined in 31CFR 1010.100(d); and includes savings and loan associations, thrift institutions, and credit unions. The customers that the bank may exempt are called “exempt persons.” An exempt person may be a bank, government agency/government authority, listed company, listed company subsidiary, eligible non-listed business, or payroll customer. A bank may, but is not required to, use this report to notify the Treasury that the bank has revoked the designation of a customer as an exempt person. ►►

Implementation Strategy

The Firm does not meet the classification of a domestic bank, savings association, thrift institution, or credit union. Therefore, the Firm is not currently required to complete and/or submit the *Department of Treasury Form 90-22.53* as a designation for exempt person(s). However, in the event the Firm is required to file a FinCEN Report 110, all reports are to be filed with FinCEN through the BSA E-Filing System.

Funds Transfers and Transmittals

All broker/dealers effecting transmittals or transfers of funds, including wire fund transfers of at least $3,000 must collect, retain and record the following information on the transmittal order:

- The name of the transmittal and recipient;
- The amount of the transmittal order;

- The identity of the recipient's financial institution; and
- The account number of the recipient.

10.04 Risk-Based Assessment of Customer Accounts

The Firm's anti-money laundering procedures are reasonably designed to determine certain associated risk-based factors when opening and/or maintaining customer accounts. In assessing the potential risks associated with its customers and/or transactions, the Firm will evaluate all areas of its business to determine certain vulnerable areas which may be subject to suspicious or potential illegal activity. Examples of certain factors which may determine the Firm's heightened scrutiny of particular customers or transactions may include the following:

- How the client became a customer with the Firm;
- The customer's past experience with the Firm;
- Whether the customer's home country is a member of FATF or is subject to adequate anti-money laundering controls in its home jurisdiction;
- The type and kind of business performed by the customer (e.g. cash intensive business);
- Whether the customer resides in, is incorporated in or operates from a jurisdiction with bank secrecy laws;
- The type of account to be opened by the Firm (e.g. individual, public, private, intermediate, foreign corporation, etc.).

10.05 Customer Identification Program (CIP)

In accordance with *Section 326 of the PATRIOT Act and relevant notice to members (NTMs),* the Firm will establish a customer identification program (CIP) that will be a part of its overall AML compliance program. The creation and implementation of the Firm's CIP shall enable the firm to form a reasonable belief that it knows the true identity of its customers.

Note: The term "customer" is defined as a person that opens a new account or an individual who opens a new account for an individual who lacks legal capacity or for an entity that is not a legal person. ("Customer" does not refer to persons who fill out account opening paperwork or who provide information necessary to establish an account, if such persons are not the accountholder as well. The definition of "customer" also does not include persons with authority over accounts.)

Section 326 of the Act requires certain minimum standards for financial institutions and their customers regarding the verification of a customer's identity in connection with the opening of an account. The regulations implementing section 326 require, at a minimum, financial institutions to implement reasonable customer identification procedures such as:

- verifying the identity of any person seeking to open an account, to the extent reasonable and practicable;
- maintaining records of the information used to verify the person's identity, including name, address, and other identifying information; and
- determining whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency.

General Due Diligence When Opening an Account

- Inquire about the source of the customer's assets and income so that the firm can determine if the inflow and outflow of money and securities is consistent with the customer's financial status;
- Gain an understanding of what the customer's likely trading patterns will be, so that any deviations from the patterns can be detected;
- Maintain records that identify the owners of accounts and their respective citizenship;
- Require customers to provide street addresses to open an account, and not simply post office addresses, or "mail drop" addresses;
- Periodically contact businesses to verify the accuracy of addresses, the place of business, the telephone, and other identifying information; and
- Periodic credit history and criminal background checks through vendor databases.

Several factors were considered in development of the Firm's CIP, such as the Firm's size, location, customer base, and overall transactional activity. As such, the Firm will consider the types of identifying information available for customers and the methods available to verify such information. The Firm's CIP sets forth certain minimum required information and suitable verification methods to be provided on an ongoing basis:

Minimum Requirements

At a minimum, the following information must be obtained from a customer prior to opening an account:

- Name;
- Date of birth, for an individual;
- Address, which will be:
    - For an individual, a residential or business street address;
    - For an individual who does not have a residential or business street address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, or the residential or business street address of a next of kin or another contact individual; or
    - For a person other than an individual (such as a corporation, partnership or trust), a principal place of business, local office or other physical location; and
- An identification number, which will be:
    - For a U.S. person, a taxpayer identification number; or
    - For a non-U.S. person, one or more of the following: a taxpayer identification number, a passport number and country of issuance, an alien identification card number, or the number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard. ►►

Implementation Strategy

Prior to opening an account, the designated supervisor will ensure that the Firm is collecting the following information for any person, entity or organization who is opening a new account and whose name is on the account:

- Name;
- Date of birth (for an individual);
- Address information, which will be a residential or business street address (for an individual), an APO or FPO number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address), or a principal place of business, local office or other physical location (for a person other than an individual); and
- Identification number, which will be a taxpayer identification number such as a driver's license or passport (for U.S. persons); or a taxpayer identification number, passport number and country of issuance, alien identification card number or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard (for non-U.S. persons).

Note: The aforementioned CIP requirements and monitoring procedures shall also apply to existing employees who open and maintain accounts at the Firm.

Regarding employee conduct, each representative of the Firm receives appropriate AML training on an annual basis and is supervised by the designated AMLCO to ensure compliance with the Firm's internal AML policies for properly identifying red flags and potential suspicious activity as well as reporting requirements. Selected non-registered employees will also receive AML training as deemed appropriate.

Note: "appropriate AML training" includes but is not limited to each registered representative attending one or more AML related training topics throughout the year. The AML related topics can be through the use of Webinars, Seminars, work books, conferences, and/or consultant presentations to maintain sufficient knowledge on AML compliance requirements, procedures and processes.

Note: In the event that a customer has applied for, but has not received, a taxpayer identification number, we will request a copy of any corresponding documentation to confirm that the application was filed before the customer opens the account and to obtain the taxpayer identification number within a reasonable period of time after the account is opened (approx. 5 days). When opening an account for a foreign business or enterprise that does not have an identification number, the designated supervisor will ensure that the Firm is requesting alternative government-issued documentation certifying the existence of the business or enterprise.

Customer Verification Methods

To the extent reasonable and practicable, the Firm will ensure that it has a reasonable belief that it knows the true identity of its customers by using risk-based procedures to verify and document the accuracy of the information it receives about its customers. The Firm will verify customer identity through the review of documentary evidence, non-documentary evidence, or both. The Firm will use documents to verify customer identity when appropriate documents are available.

Documentary Methods of Verification

The Firm will conduct its own risk-based analysis of the types of documents that it believes will enable it to verify the true identities of its customers. Examples of documents that the Firm may use for verification include:

- For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and

- For a person other than an individual (such as a corporation, partnership, or trust), documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or a trust instrument.

Non-Documentary Methods of Verification

The Firm may implement non-documentary methods of verification under one or more of the following circumstances:

- When an individual is unable to present an unexpired government-issued identification document that bears a photograph or other similar safeguard;
- When the Firm is not familiar with the documents currently present;
- When the account is opened without obtaining documents as specified under documentary methods;
- When the customer opens an account without appearing in person at the Firm;
- When the Firm is otherwise presented with circumstances that increase the risk that the Firm will be unable to verify the true identity of a customer through documents; or
- When the Firm is presented with identification documents that may appear questionable, suspicious or otherwise invalid.

Specific Non-Documentary Methods to be Used

- Contacting the customer;
- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a customer reporting agency, public database, or other relevant source;
- Checking references with other financial institutions; or
- Obtaining a financial statement.

In addition to the requirements for obtaining and maintaining certain customer information, the Firm will make all reasonable efforts to perform due diligence procedures on the various types of accounts that the Firm maintains with its customers in accordance with "Know Your Customer" provisions. ►►

Implementation Strategy

The designated AMLCO contact person shall ensure that the Firm has a reasonable belief that it knows the true identity of its customers through the used of customer identification and verification procedures. As a result, the Firm may request documentary evidence, non-documentary evidence, or both as means of verifying customer identification. In the event that customer appears in person, *documentary verification methods* will be used; However, *non-documentary evidence* will be used under one or more of the following circumstances:

- When an individual in unable to present an un-expired government-issued identification document that bears a photograph or other similar safeguard;
- When the Firm is not familiar with the documents currently present;
- When the account is opened without obtaining documents as specified under documentary methods;
- When the customer opens an account without appearing in person:
- When the Firm is otherwise presented with circumstances that increase the risk that the Firm will be unable to verify the true identity of a customer through documents; or
- When the Firm is presented with identification documents that may appear questionable, suspicious or otherwise invalid.

Specific non-documentary verification methods to be used may include:

- contacting the customer;
- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a customer reporting agency, public database, or other relevant source;
- Checking references with other financial institutions; or
- Obtaining a financial statement.

The totality of documentary and/or non-documentary information gathered from the prospective or existing client will ultimately determine the approval of a customer account. The Firm may attempt to obtain more than one type of documentary verification and may use a variety of methods to verify the identity of a customer, especially when the Firm does not have the ability to examine the original documents. On an as-needed basis, the designated supervisor shall consistently monitor and evaluate new and existing client account information for potential risk to the Firm. All relevant customer account information will be reviewed and maintained in each customer account file for research and reference purposes.

Note: The Firm is not required to ensure the validity of documents. Once the Firm obtains and verifies the identity of a customer through a document, such as a driver's license or passport, a firm is not required to take steps to determine whether the document has been validly issued. A firm may rely on a government-issued identification as verification of a customer's identity. If, however, a firm notes that the document shows some obvious form of fraud, the firm must consider that factor in determining whether it can form a reasonable belief that it knows the customer's true identity.

Additional or Enhanced Verification Procedures

Although the Firm is able to adequately verify the majority of customers through documentary and non-documentary methods, there may be certain instances where such methods may be inadequate or insufficient. As a result, the Firm may choose to prescribe additional verification procedures for certain accounts that may be associated with heightened risk (e.g. accounts opened in the name of a corporation, partnership or trust that are created or conduct substantial business in jurisdictions that have been designated as a primary money laundering concern or as a non-cooperative by an international body).

Lack of Verification

In the event that the Firm cannot form a reasonable belief that it knows the true identity of a particular customer, the Firm will NOT open an account for such person, nor will it conduct any transactions while it attempts to verify the true identity of the person.

Notice to Customers

The Firm's CIP will provide its customers with adequate notice that it is requesting information to verify their identities. The notice will briefly describe the identification requirements of this section n a manner reasonably designed to ensure that a customer is able to view the notice, or is otherwise given notice, before opening an account. For example, depending upon the manner in which the account is opened, the Firm may have the option of posting a notice in its office or on its website, include the notice on its account applications or use any other form of oral or written notice. ►►

Implementation Strategy

The Firm shall provide proper notification of its CIP identification and verification requirements in a manner that is reasonably designed to ensure that a customer views the notice *before* opening an account with the Firm. The Firm may post such a notification through one or more methods:

- Open display in its principal place of business;
- On the Firm's Web site;
- On the Firm's New Account Applications;
- Other written disclosures.

The notification may read as follows:

"IMPORTANT INFORMATION ABOUT PROCEDURES FOR OPENING A NEW ACCOUNT. To help the government fight the funding of terrorism and money-laundering activities, and to verify your identity, federal law requires American Investors Company (AIC) to obtain your name, date of birth, address, and a government-issued identification number before opening your account. In certain circumstances, AIC may obtain and verify this information with respect to any person(s) authorized to effect transactions in an account. For certain entities, such as trusts, estates, corporations, partnerships, or other organizations, identifying documentation is also required. Your account may be restricted and/or closed if AIC cannot verify this information. AIC will not be responsible for any losses or damages (including but not limited to lost opportunities) resulting from any failure to provide this information, or from any restriction placed upon, or closing of, your account."

FinCEN Customer Due Diligence (CDD) Rule

FinCEN issued the CDD Rule to amend existing BSA regulations in order to clarify and strengthen customer due diligence requirements for certain financial institutions. The CDD Rule outlines explicit customer due diligence requirements and imposes a new requirement for these financial institutions to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions. The new CDD Rule applies to all financial institutions which includes federally regulated banks and federally insured credit unions, mutual funds, brokers or dealers in securities, futures commission merchants, and introducing brokers in commodities. The Rule will apply to all new accounts

opened at a covered financial institution by a legal entity customer on or after the May 11, 2018 applicability date.

Requirements of the CDD Rule

The CDD Rule requires covered financial institutions to establish and maintain written procedures that are reasonably designed to identify and verify the beneficial owners of legal entity customers. These procedures must enable the institution to identify the beneficial owners of each customer at the time a new account is opened, unless the customer is otherwise excluded or the account is exempted. Also, the procedures must establish risk-based practices for verifying the identity of each beneficial owner identified to the covered financial institution, to the extent reasonable and practicable. The procedures must contain the elements required for verifying the identity of customers that are individuals under applicable customer identification program ("CIP") requirements.

The CDD Rule amends the AML program requirements for each covered financial institution to explicitly require covered institutions to implement and maintain appropriate risk based procedures for conducting ongoing customer due diligence, to include:

- understanding the nature and purpose of the customer relationships; and
- conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.

The CDD Rule requires that the procedures, at a minimum, contain the same elements as required for verifying the identity of customers that are individuals under the applicable CIP rule. However, financial institutions may use photocopies or other reproductions of identification documents in the case of documentary verification.

Focus on Beneficial Owners

Covered financial institutions must collect information on individuals who are beneficial owners of a legal entity customer in addition to the information they are required to collect on the customer under the CIP requirement.

The Rule defines beneficial owner as each of the following:

- each individual, if any, who, directly or indirectly, owns 25% or more of the equity interests of a legal entity customer (i.e., the ownership prong); and
- a single individual with significant responsibility to control, manage, or direct a legal entity customer, including an executive officer or senior manager (e.g., a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, or Treasurer); or any other individual who regularly performs similar functions (i.e., the control prong). This list of positions is illustrative, not exclusive, as there is significant diversity in how legal entities are structured.

Note: The Rule defines a legal entity customer as a corporation, limited liability company, other entity created by the filing of a public document with a Secretary of State or similar office, a general partnership, and any similar entity formed under the laws of a foreign jurisdiction that opens an account. The definition also includes limited partnerships, business trusts that are created by a filing with a state office, and any other entity created in this manner. A legal entity customer does not include sole proprietorships, unincorporated associations, or natural persons opening accounts on their own behalf.

Note: FinCEN's expectation is that the control person identified must be a high-level official in the legal entity, who is responsible for how the organization is run, and who will have access to a range of information concerning the day-to-day operations of the company. The list of positions is illustrative, not exclusive.

Information Collected for Beneficial Owners

As with CIP for individual customers, covered financial institutions must collect from the legal entity customer the name, date of birth, address, and social security number or other government identification number (passport number or other similar information in the case of foreign persons) for individuals who own 25% or more of the equity interest of the legal entity (if any), and an individual with significant responsibility to control/manage the legal entity at the time a new account is opened.

Nominee Owners

FinCEN intends that the legal entity customer identify its ultimate beneficial owner or owners and not "nominees" or "straw men." FinCEN reiterates that it is the responsibility of the legal entity customer to identify its ultimate beneficial owners and that the financial institution may rely upon the information provided, unless the institution has reason to question its accuracy.

Exemptions and Limitations on Exemptions

Subject to certain limitations, covered financial institutions are also not required to identify and verify the identity of the beneficial owner(s) of a legal entity customer when the customer opens any of the following four categories of accounts:

- accounts established at the point-of-sale to provide credit products, solely for the purchase of retail goods and/or services at these retailers, up to a limit of $50,000
- accounts established to finance the purchase of postage and for which payments are remitted directly by the financial institution to the provider of the postage products
- accounts established to finance insurance premiums and for which payments are remitted directly by the financial institution to the insurance provider or broker; and
- accounts established to finance the purchase or lease of equipment and for which payments are remitted directly by the financial institution to the vendor or lessor of this equipment.

These exemptions will not apply under either of the following two circumstances:

- if the accounts are transaction accounts through which a legal entity customer can make payments to, or receive payments from, third parties.
- if there is the possibility of a cash refund for accounts opened to finance purchase of postage, insurance premium, or equipment leasing. If there's the possibility of a cash refund, the financial institution must identify and verify the identity of the beneficial owner(s) either at the initial remittance, or at the time such refund occurs

Exclusions from the Definition of Legal Entity Customer

The CDD Rule excludes from the definition of legal entity customer certain entities that are subject to Federal or State regulation and for which information about their beneficial ownership and management is available from the Federal or State agencies, such as:

- Financial institutions regulated by a Federal functional regulator or a bank regulated by a State bank regulator;

- Certain exempt persons for purposes of the currency transactions reporting obligations:
    - A department or agency of the United States, of any State, or of any political subdivision of a State;
    - Any entity established under the laws of the United States, or any State, or of any political subdivision of any State, or under an interstate compact;
    - Any entity (other than a bank) whose common stock or analogous equity interests are listed on the New York, American, or NASDAQ stock exchange;
    - Any entity organized under the laws of the United States or of any State at least 51% of whose common stock or analogous equity interests are held by a listed entity
- Issuers of securities registered under section 12 of the Securities Exchange Act of 1934 (SEA) or that is required to file reports under 15(d) of that Act;
- An investment company, as defined in section 3 of the Investment Company Act of 1940, registered with the U.S. Securities and Exchange Commission (SEC);
- An SEC-registered investment adviser, as defined in section 202(a)(11) of the Investment Advisers Act of 1940;
- An exchange or clearing agency, as defined in section 3 of the SEA, registered under section 6 or 17A of that Act;
- Any other entity registered with the SEC under the SEA;
- A registered entity, commodity pool operator, commodity trading advisor, retail foreign exchange dealer, swap dealer, or major swap participant, defined in section 1a of the Commodity Exchange Act, registered with the Commodity Futures Trading Commission;
- A public accounting firm registered under section 102 of the Sarbanes-Oxley Act

Additional regulated entities:

- A bank holding company, as defined in section 2 of the Bank Holding Company Act of 1956 (12 USC 1841) or savings and loan holding company, as defined in section 10(n) of the Home Owners' Loan Act (12 USC 1467a(n));
- A pooled investment vehicle operated or advised by a financial institution excluded from the definition of legal entity customer under the final CDD rule;
- An insurance company regulated by a State;
- A financial market utility designated by the Financial Stability Oversight Council under Title VIII of the Dodd-Frank Wall Street Reform and Customer Protection Act of 2010;

Excluded Foreign Entities:

- A foreign financial institution established in a jurisdiction where the regulator of such institution maintains beneficial ownership information regarding such institution;
- A non-U.S. governmental department, agency or political subdivision that engages only in governmental rather than commercial activities; and
- Any legal entity only to the extent that it opens a private banking account subject to 31 CFR 1010.620

Note: Trusts included in the definition of legal entity customer. The definition of legal entity customers only includes statutory trusts created by a filing with the Secretary of State or similar office. Otherwise, it does not include trusts. This is because a trust is a contractual arrangement between the person who provides the funds or other assets and specifies the terms (i.e., the grantor/settlor) and the person with control over the assets (i.e., the trustee), for the benefit of those named in the trust deed (i.e., the beneficiaries). Formation of a trust does not generally require any action by the state.

Customer Due Diligence Requirements for Financial Institutions; FIN-2016-G003; Issued: July 19, 2016; Applicability Date May 11, 2018

Implementation Strategy

For all new accounts opened for a legal entity customer on or after the May 11, 2018 applicability date, the Firm will ensure that applicable CDD requirements will be met. The Firm will collect information on individuals who are considered beneficial owners of a legal entity customer in addition to the information collected on the customer under the CIP requirement. Information collected will include the name, date of birth, address, and social security number or other government identification number (passport number or other similar information in the case of foreign persons) for individuals who own 25% or more of the equity interest of the legal entity (if any), and an individual with significant responsibility to control/manage the legal entity at the time a new account is opened.

Comparison with Government Lists

The Firm shall screen its customers to determine whether a customer appears on any list of known or suspected terrorists or terrorist organizations issued by any Federal government agency and designated as such by Treasury in consultation with the Federal functional regulators. Such a determination shall be made within a reasonable period of time after the account is opened, or earlier if required by another Federal law or regulation or Federal directive issued in connection with the applicable list, and the Firm shall follow all Federal directives issued in connection with such lists. ►►

Implementation Strategy

Not applicable at this time. The Treasury and the Federal functional regulators have not yet designated any government lists.

10.06 U.S. Correspondent Accounts with Foreign Shell Banks

In Accordance with *Section 313 of the PATRIOT Act*, the Firm shall not establish, maintain, administer, or manage a correspondent account in the United States for, or on behalf of, a foreign bank that does not have a physical presence in any country.

Prevention of Indirect Service to Foreign Shell Banks

The Firm shall take reasonable steps to ensure that any correspondent account established, maintained, administered, or managed by the Firm in the United States for a foreign bank is not being used by that foreign bank to indirectly provide banking services to another foreign bank that does not have a physical presence in any country.

Certain exceptions may apply if the foreign bank (i) is an affiliate of a depository institution, credit union, or foreign bank that maintains a physical presence in the United States or a foreign country, as applicable; and (ii) is subject to supervision by a banking authority in the country regulating the affiliated depository institution, credit union, or foreign bank.

Maintenance of Records in the U.S.

In the event that the Firm maintains a correspondent account in the U.S. for a foreign bank, the Firm shall be required to maintain records in the U.S. identifying the owners of such foreign bank and the name and address of a person who resides in the United States and is authorized to accept service of legal process for records regarding the correspondent account.

Law Enforcement Request

Upon receipt of a written request from a Federal law enforcement officer for information required to be maintained for any U.S. correspondent accounts with foreign banks, the Firm shall provide the information to the requesting officer no later than seven (7) days after receipt of the request.

Termination of Correspondent Relationships with a Foreign Bank

The Firm shall terminate any correspondent relationship with a foreign bank no later than ten (10) business days after receipt of written notice from the Secretary or the Attorney General (in each case, after consultation with the other) that the foreign bank has failed (i) to comply with a summons or subpoena; or (ii) to initiate proceedings in a United States court contesting such summons or subpoena. ►►

Implementation Strategy

The Firm does not establish, maintain, administer, or manage correspondent accounts in the United States for, or on behalf of, a foreign bank that does not have a physical presence in any country. However, in the event that the Firm did open and/or manage such accounts, the designated compliance officer would ensure that the Firm is identifying and verifying the information of all owners by requesting relevant identification information as specified in the Due Diligence for Certain Types of Accounts. Additionally, in accordance with record maintenance requirements, the Firm shall be required to maintain records in the U.S. identifying the owners of such foreign bank and the name and address of a person who resides in the United States and is authorized to accept service of legal process for records regarding the correspondent account.

10.07 Private Banking Accounts/Foreign Officials

Firms must have a due diligence program that is reasonably designed to detect and report any known or suspected money laundering conducted through or involving any private banking account maintained by or on behalf of a non-U.S. person, as well as the existence of the proceeds of foreign corruption in any such account. This requirement applies to all private banking accounts for non-U.S. persons, regardless of when they were opened. Accounts requested or maintained by or on behalf of "senior foreign political figures" (including their family members and close associates) require enhanced scrutiny.

A "private banking" account is an account (or any combination of accounts) that requires a minimum aggregate deposit of $1,000,000, is established for one or more individuals, and is assigned to or administered or managed by, in whole or in part, an officer, employee, or agent of a financial institution acting as a liaison between the financial institution and the direct or beneficial owner of the account.

A "senior foreign political figure" includes a current or former senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not), a senior official of a major foreign political party, or a senior executive of a foreign government-owned commercial enterprise; a corporation, business, or other entity formed by or for the benefit of any such individual; an immediate family member of such an individual; or any individual publicly known (or actually known by the firm) to be a close personal or professional associate of such an individual. ►►

Implementation Strategy

The Firm does not have any "private banking" accounts at this time. However, in the event that the Firm maintained "private banking" accounts, the designated supervisor will ensure that the Firm periodically reviews its accounts to determine

whether to conduct due diligence on such accounts. This due diligence will include, at a minimum, (i) ascertaining the identity of all nominal holders and holders of any beneficial ownership interest in the account (including information on those holders' lines of business and sources of wealth); (ii) ascertaining the source of funds deposited into the account; (iii) ascertaining whether any such holder may be a senior foreign political figure; and (iv) detecting and reporting, in accordance with applicable law and regulation, any known or suspected money laundering and/or use of the proceeds of foreign corruption. Decisions to open accounts for senior foreign political figures should be approved by senior management.

10.08 Review of Specially Designated Nationals/ Blocked Persons as Listed by OFAC

As and when deemed appropriate, the Firm will review all economic and trade related sanctions against targeted foreign countries, terrorism sponsoring organizations and current lists of Specially Designated Nationals and Blocked Persons as administered and enforced by the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC"). OFAC acts under Presidential wartime and national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze foreign assets under U.S. jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.

Executive Order 13224 (Blocking Property and Prohibiting Transactions with Persons who Commit, Threaten to Commit, or Support Terrorism)

For example, except to the extent required by *section 203(b) of IEEPA (50 U.S.C. 1702(b)),* or provided in regulations, orders, directives, or licenses that may be issued pursuant to this order, and notwithstanding any contract entered into or any license or permit granted prior to the effective date of this order, all property and interests in property of the following persons that are in the U.S. or that hereafter come within the U.S., or that hereafter come within the possession or control of U.S. persons are blocked:

- foreign persons listed in the Annex to this order;
- foreign persons determined by the Secretary of State, in consultation with the Secretary of the Treasury and the Attorney General, to have committed, or to pose a significant risk of committing, acts of terrorism that threaten the security of U.S. nationals or the national security, foreign policy, or economy of the United States;
- persons determined by the Secretary of the Treasury, in consultation with the Secretary of State and the Attorney General, to be owned or controlled by, or to act for or on behalf of those persons listed in the Annex to this order;
- except as provided in section 5 of this order and after such consultation, if any, with foreign authorities as the Secretary of State, in consultation with the Secretary of the Treasury and the Attorney General, deems appropriate in the exercise of his discretion, persons determined by the Secretary of the Treasury, in consultation with the Secretary of State and the Attorney General. ►►

Implementation Strategy

Upon each account opening, the designated supervisor or his designee will perform periodic reviews of the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") list of Specially Designated Nationals and Blocked Persons to ensure that potential customers and existing customers are not prohibited persons or entities and are not from embargoed countries or regions before transacting any business

with them. The review shall be conducted through the OFAC Web site (http://www.ustreas.gov/ofac/) or FINRA's site (http://apps.finra.org/rulesregulation/ofac/1/Default.aspx). Evidence of each OFAC review will be recorded on the new account form and maintained as confirmation of match/no- match status. The Firm's designated clearing firm will perform OFAC reviews on accounts held with the clearing firm. Exception reports will be reviewed by the Firm to identify any prohibited person or entities.

Additionally, pursuant to the information contained in Executive Order 13224 and/or other relevant sanctions, the Firm shall immediately freeze any/all related accounts and prohibit future transactions with persons who are suspected of terrorist activities. Additional actions shall include the completion of a suspicious activity report (SAR-SF) and/or immediate notification to authorities. Any and all actions taken on the part of the Firm to freeze such accounts will be properly documented and evidenced as reviewed.

OFAC's Russia-related sanctions

On February 24, 2022, the Department of the Treasury announced additional sanctions against Russia. As part of these measures, the Department of the Treasury's Office of Foreign Assets Control (OFAC) issued Directive 2 Under Executive Order 14024: Prohibitions Related to Correspondent or Payable-Through Accounts and Processing of Transactions involving Certain Foreign Financial Institutions, as well as Directive 3 Under Executive Order 14024: Prohibitions Related to New Debt and Equity of Certain Russia-related Entities.

Treasury stated the OFAC measures target "Russia's two largest financial institutions, Public Joint Stock Company Sberbank of Russia (Sberbank) and VTB Bank Public Joint Stock Company (VTB Bank)," as well as three other major Russian financial institutions, Otkritie, Novikom and Sovcom. These sanctions include numerous subsidiaries of Sberbank, VTB Bank, Otkritie and Sovcom.

OFAC also "expanded Russia-related debt and equity restrictions to additional key aspects of Russia's economy" and issued Directive 3 "to prohibit transactions and dealings by U.S. persons or within the United States in new debt of longer than fourteen days maturity and new equity of Russian state-owned enterprises, entities that operate in the financial services sector of the Russian Federation economy, and other entities determined to be subject to the prohibitions in this directive.

In addition, "(p)ursuant to E.O. 14024, OFAC identified the following 11 Russian entities as being owned or controlled by, or having acted or purposed to act for or on behalf of, directly or indirectly, the GoR:"

- Sberbank,
- Gazprombank Joint Stock Company,
- Joint Stock Company Russian Agricultural Bank,
- Public Joint Stock Company Gazprom,
- Public Joint Stock Company Gazprom Neft,
- Public Joint Stock Company Transneft,
- Public Joint Stock Company Rostelecom,
- Public Joint Stock Company RusHydro,
- Public Joint Stock Company Alrosa,
- Joint Stock Company Sovcomflot, and
- Open Joint Stock Company Russian Railways

Further pursuant to E.O. 14024, "OFAC identified the following three Russian entities for operating or having operated in the financial services sector of the Russian Federation economy:"

- Joint Stock Company Alfa-Bank,

- Credit Bank of Moscow Public Joint Stock Company, and
- Sberbank.

To ensure that these sanctions and prohibitions have an impact on the intended targets and to minimize unintended consequences on third parties, OFAC has also issued several general licenses in connection with these actions.

The sanctions announced on February 24, 2022, also target Russian elites close to Russian President Vladimir Putin. These sanctions target:

- Sergei Sergeevich Ivanov (son of Sergei Borisovich Ivanov),
- Andrey Patrushev (son of Nikolai Platonovich Patrushev),
- Ivan Igorevich Sechin (son of Igor Ivanovich Sechin),
- Alexander Aleksandrovich Vedyakhin, and
- Andrey Sergeyevich Puchkov (Puchkov) and Yuriy Alekseyevich Soloviev (Soloviev) and other related parties to Puchkov and Soloviev such as Limited Liability Company Atlant S and Limited Liability Company Inspira Invest A. and Soloviev's wife, Galina Olegovna Ulyutina.

On February 22, the Department of the Treasury announced a series of sanctions pursuant to Executive Order 14024 "in response to actions in the Donetsk and Luhansk regions." The Department's press release stated the sanctions target "Russia's ability to finance aggression against its neighbors by sanctioning the Corporation Bank for Development and Foreign Economic Affairs Vnesheconombank (VEB) and Promsvyazbank Public Joint Stock Company (PSB), along with 42 of their subsidiaries."

In addition, the press release noted that, "Treasury is also designating influential Russians and their family members in Putin's inner circle believed to be participating in the Russian regime's kleptocracy, including the Chairman and CEO of PSB." These sanctions target:

- Denis Aleksandrovich Bortnikov (son of Aleksandr Vasilievich Bortnikov),
- Petr Mikhailovich Fradkov, and
- Vladimir Sergeevich Kiriyenko (son of Sergei Vladilenovich Kiriyenko).

Treasury also announced "increased restrictions on dealings in Russia's sovereign debt" pursuant to Executive Order 14024 that extend "existing sovereign debt prohibitions to cover participation in the secondary market for bonds issued after March 1, 2022 by the Central Bank of the Russian Federation, the National Wealth Fund of the Russian Federation, or the Ministry of Finance of the Russian Federation."

On February 21, 2022, President Biden issued an Executive Order on Blocking Property of Certain Persons and Prohibiting Certain Transactions With Respect to Continued Russian Efforts to Undermine the Sovereignty and Territorial Integrity of Ukraine.

Among its elements, the Executive Order prohibits certain activities, such as:

- "new investments in the so-called DNR and LNR regions of Ukraine or such other regions of Ukraine as may be determined by the Secretary of the Treasury, in consultation with the Secretary of State (collectively the 'Covered Regions'), by a United States person, wherever located;"

- "the importation into the United States, directly or indirectly, of any goods, services, or technology from the Covered Regions;"

- "the exportation, reexportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, wherever located, of any goods, services, or technology to the Covered Regions;" and

- “any approval, financing, facilitation, or guarantee by a United States person, wherever located, of a transaction by a foreign person where the transaction by that foreign person would be prohibited by this section if performed by a United States person or within the United States.”

In addition, the Executive Order states, "(a)ll property and interests in property that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person (including any foreign branch) of the following persons are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in: any person determined by the Secretary of the Treasury, in consultation with the Secretary of State:”

- “to operate or have operated since the date of this order in the Covered Regions;”

- “to be or have been since the date of this order a leader, official, senior executive officer, or member of the board of directors of an entity operating in the Covered Regions;”

- “to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to this order;” and

- “to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, any person whose property and interests in property are blocked pursuant to this order.”

The prohibitions described in the previous paragraph “include, but are not limited to”:

- “the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any person whose property and interests in property are blocked pursuant to this order;” and

- “the receipt of any contribution or provision of funds, goods, or services from any such person.”

The Executive Order also prohibits "any transaction that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions” and “any conspiracy formed to violate any of the prohibitions” set forth in the Executive Order.

Implementation Strategy

In light of recent events, the Firm will monitor its existing customer accounts, account opening processes and ongoing transactional activity to ensure that the Firm maintains proper controls and restrictions related to Russian entities for operating or having operated in the financial services sector of the Russian Federation economy, and specific persons in accordance with Directive 2 Under Executive Order 14024: Prohibitions Related to Correspondent or Payable-Through Accounts and Processing of Transactions involving Certain Foreign Financial Institutions, as well as Directive 3 Under Executive Order 14024: Prohibitions Related to New Debt and Equity of Certain Russia-related Entities and Executive Order on Blocking Property of Certain Persons and Prohibiting Certain Transactions With Respect to Continued Russian Efforts to Undermine the Sovereignty and Territorial Integrity of Ukraine.

The review will be conducted through the OFAC Web site and/or via selected vendor (if applicable). Evidence of each OFAC review will be recorded on the new account form and maintained as confirmation of match/no- match status.

10.09 Reliance on another Financial Institution

The Firm may reasonably rely on the performance of another financial institution's CIP (including an affiliate) with respect to any customer of the Firm that is opening an account or has established an account or similar business relationship with another financial institution to provide or engage in services, dealings, or other financial transactions, provided that:

- Such reliance is reasonable under the circumstances;
- The other financial institution is also subject to the AML rules and regulated by a "Federally functional regulator;"
- The other financial institution enters into a contract requiring it to certify annually to the Firm that it has implemented its AML program, and that it will perform specified requirements of the Firm's CIP.

10.10 Use of Clearing Firms

Within the securities industry, there is a large number of introducing broker/dealer firms which utilize clearing brokers to clear securities transactions on their behalf. In these and other such similar cases, it is generally understood that "Know Your Customer" rules and other related suitability requirements are the responsibility of the introducing firm. Such responsibilities include taking reasonable steps to know the customer as well as the customer's investment experience and overall investment objectives.

The Clearing Agreement

With the recent implementation of the *USA PATRIOT Act*, the Firm will review its clearing agreement for information on any/all anti-money laundering procedures. The focus of such a review will be on any disclosure or reference to the allocation of anti-money laundering responsibilities between the introducing firm and its assigned clearing broker to include the filing of currency transactions and suspicious activity reports.

Reporting Requirements for Introducing vs. Clearing Firms

Securities transactions may be conducted by broker/dealers that clear their own transactions or by introducing brokers that rely on another firm to clear the transactions. Although the responsibility and obligation to identify and report a suspicious transaction rests with each broker/dealer involved in the transaction, only one SAR-SF is required to be filed, provided that the report includes all relevant facts concerning the transaction. In this case, the introducing and clearing broker/dealer will remain in constant communication for the purposes of sharing information about the transaction in order to determine which firm will file the SAR-SF.

In cases where such communication is appropriate and results in a filing of a SAR-SF, the broker/dealer filing the SAR-SF may provide a copy of such report to the other broker/dealer with which it shared such communications. However, there are certain instances of communication between broker/dealers about suspicious transactions and the subsequent filing of a SAR-SF that would be inappropriate. For example, a broker/dealer that suspects that it is required to report another broker/dealer or one of its employees as the subject of a SAR-SF would be prohibited from notifying the other broker/dealer that a SAR-SF was filed.

Additionally, *Section 314(b) of the USA Patriot Act* permits two (2) or more financial institutions and any association of financial institutions upon notice to the Treasury to "share information with one another regarding individuals, entities, organizations, and countries suspected of possible terrorist or money laundering activities."

Availability of Exception Reports

If necessary, the introducing firm may reasonably request certain exception reports that might assist in the review and analysis of specific or patterned transactional activity on the part of the customer. Examples of exception data may include information on deposit and trading activity which may be a possible source for indicating potential anti-money laundering activity. ►►

Implementation Strategy

The designated supervisor shall maintain periodic correspondence with the Firm's designated clearing firm in order to obtain exception reports or other relevant and up-to-date data and information that would assist the Firm in increasing its anti-money laundering efforts. Any and all reports and documentation on anti-money laundering issues that are received by the designated clearing firm will be reviewed and maintained in a properly labeled file.

10.11 Training on Anti-Money Laundering Procedures

All new and existing employees of broker/dealer firms shall receive ongoing training relating to anti-money laundering procedures, including the detection of unusual or suspicious transactions and compliance with all relevant federal rules and regulations and reporting requirements. Such anti-money laundering training shall include all relevant internal documentation such as handouts, pamphlets, manuals, the Firm's Code of Ethics and/or Code of Conduct, and other content-specific materials.

Anti-Money Laundering Training Needs

In the assessment and development of the Firm's current Anti-Money Laundering training needs, the following factors were considered:

- Size and scope of the Firm's investment focus and activity;
- Critical issues concerning internal compliance or legal matters;
- Feedback from management and registered personnel;
- Feedback from registered personnel and other employees;
- Independent audit reviews of the Firm's anti-money laundering program;
- Consideration of regulatory requirements.

Anti-Money Laundering Training Focus

The Firm's main focus shall remain in the areas of "Know Your Customer" policies and procedures; potential indicators of suspicious activity; the rules and regulations for reporting currency transactions, transportation of monetary instruments and suspicious activity; procedures for reporting such suspicious transactions and/or activity; and the civil and criminal penalties associated with money laundering.

As previously stated, the Firm will periodically review all economic and trade related sanctions against targeted foreign countries, terrorism sponsoring organizations and current lists of Specially Designated Nationals and Blocked Persons as administered and enforced by the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC"). OFAC acts under Presidential wartime and national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze foreign assets under U.S. jurisdiction. Many of the

sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.

Note: For a complete and up-to-date listing of targeted foreign countries, terrorism sponsoring organizations and OFAC's list of Specially Designated Nationals and Blocked Persons, please visit OFAC's Web site at (http://www.ustreas.gov/ofac/).

Anti-Money Laundering Training Format

The Firm has elected to present its Anti-Money Laundering Training Program utilizing one or more of the following formats: (a) Direct Participation in Seminars/Lectures; (b) Live Presentations/Classroom Instruction; (c) On-Line Training Programs or Courses; (d) Educational Videos; (e) Miscellaneous Educational Materials/ Self-Paced Study Program.

In addition, the Firm may distribute bulletins or other guidance documents to all employees, or to specific groups of registered representatives as appropriate (i.e. registered persons in particular branch locations or specific departments such as Compliance, Legal, Audit, Cashiering, Margin, or Operations). ►►

Implementation Strategy

The Firm will develop an internal training program that may include the use of classroom training (periodic meetings) and the distribution of On-line/ Internet reference materials and other misc. educational materials. The Firm will initially provide each associated person with a copy of the Firm's anti-money laundering procedures for review. Additionally, the designated AML contact person will review the following Web sites for up-to-date information on anti-money laundering issues and distribute up-dates on an as-needed basis:

1. U.S. Department of Treasury (http://www.treas.gov)
2. *Office of Foreign Assets Control (OFAC) (http://www.ustreas.gov/ofac/)
3. Financial Action Task Force (http://www1.oecd.org/fatf/)
4. Financial Crimes Enforcement Network (FinCEN) (http://www.fincen.gov/)

**Note: For a complete and up-to-date listing of targeted foreign countries, terrorism sponsoring organizations and OFAC's list of Specially Designated Nationals and Blocked Persons, please visit OFAC's Web site at (http://www.ustreas.gov/ofac/).*

10.12 Books and Records Requirements for AML Procedures

It is the Firm's policy to retain all books and records relating to its Anti-Money Laundering Procedures in accordance with the *Bank Secrecy Act* (BSA), *Federal Funds Transfer Rules*, and other such rules promulgated by the Firm's regulators, including the Treasury Department, the Securities and Exchange Commission, and all applicable self-regulatory organization (SRO) rules and regulations.

The Firm must make a record of the identifying information obtained about each customer. However, rather than requiring copies of verification documents, the Firm's records must include a description of any document that the it relied on to verify the identity of its customer, noting the type of document, any identification number contained in the document, the place of issuance, and the issuance and expiration dates, if any. With respect to non-documentary verification, the final rule now requires the records to include "a description" of the methods and results of any measures undertaken to verify the identity of the customer. The Firm is also required to record the resolution of any substantive discrepancy discovered when verifying the identifying information obtained.

In addition to the specific records as stated above, all relevant training materials and outlines, as well as detailed records reflecting how the Firm's Anti-Money Laundering Training Program was developed, implemented, and administered, will be retained as part of its books and records requirements under *Rules 17a-3* and *17a-4* of the *Securities Exchange Act of 1934*. At a minimum, the Firm shall maintain all records and other pertinent documentation relating to anti-money laundering procedures for a period of five (5) years. ►►

Implementation Strategy

At a minimum, the Firm will maintain records and other pertinent documentation relating to its anti-money laundering program for a period of five (5) years. More specifically, the Firm will maintain all relevant information obtained from each customer for a period of five years after the date the account is closed. Those records that verify a customer's identity will be maintained for a period of five years from the date the record is made.

10.13 Independent Audit Program

In accordance with *Section 352 of the USA PATRIOT Act*, the Firm will establish an independent audit program that is reasonably designed to assess and determine the Firm's overall compliance with its prescribed anti-money laundering policies and procedures. In the course of constructing the anti-money laundering audit program, it shall be the Firm's discretion in determining the use of an internal or external auditing process, or both.

In accordance with certain amendments to *FINRA Rule 3310,* the amended rule language establishes an expectation that, for most firms, the independent test should be performed at least once each calendar year. The new rule language, however, allows firms that do not execute transactions for customers or otherwise hold customer accounts or act as an introducing broker with respect to customer accounts to test once every two years (on a calendar-year basis) rather than on an annual basis.

Qualifications for conducting Independent Testing Function

FINRA Rule 3310 clarifies certain types of individuals who FINRA would not consider to be "independent," and, hence, not eligible to perform the required independent testing. As an initial matter, *FINRA Rule 3310* clarifies that the person conducting the independent test must have a working knowledge of applicable requirements under the Bank Secrecy Act and its implementing regulations. *FINRA Rule 3310* further clarifies that, to ensure sufficient separation of functions for independence purposes, the testing cannot be conducted by the AML compliance person(s) designated in *FINRA Rule 3310*, by any person who performs the AML functions being tested or by any person who reports to any of these persons. ►►

Implementation Strategy

The Firm will develop and implement an internal audit process to review the Firm's overall compliance with its prescribed anti-money laundering policies and procedures. As a result, the designated AML contact person or an independent outside person/consultant will conduct an independent test of the Firm's AML operational procedures and overall compliance within each calendar year. Any finding and/or recommendations will be submitted to CCO and AMLCO in the form of an AML Report. All AML Reports detailing the findings, recommendation and/or results of the independent test will be maintained in a separate audit file for record keeping purposes. The AMLCO or will ensure that each AML Report resulting from an annual inspection is completed each calendar year. Each AML Report will be signed as evidence of review and approval.

However, in the event the Firm does not execute transactions for customers or otherwise hold customer accounts or act as an introducing broker with respect to customer accounts, the Firm may elect to conduct its AML test every other year in accordance with amended FINRA Rule 3011(c) and IM-3011-1.

10.14 Regulatory Examination and Enforcement

Overall compliance with the aforementioned rules and regulations shall be examined by the Department of the Treasury, through FinCEN or other designated and/or authorized appointees, under the terms of the Bank Secrecy Act (BSA). Any and all reports filed under this section shall be made available to an SRO registered with the SEC examining a broker/dealer for compliance with BSA and other relevant anti-money laundering rules and regulations. Failure to comply with such requirements may constitute a violation of the reporting rules of the BSA.

10.15 Notification for Purposes of Section 314(b) of the USA PATRIOT Act

On September 26, 2002, FinCEN issued a final rule regarding information sharing among financial institutions and federal government law enforcement agencies for the purpose of identifying, preventing, and deterring money laundering and terrorist activity. In general, a financial institution may share information with another financial institution about those suspected of terrorism or money laundering through the use of a FinCEN notice.

This FinCEN notice allows the Firm to engage in the sharing of information with other financial institutions or associations of financial institutions regarding individuals, entities, organizations, and countries, as permitted by section 314(b) of the USA PATRIOT Act of 2001 (Public Law 107-56) and the implementing regulations of the Department of the Treasury, Financial Crimes Enforcement Network (31 CFR 103.110). ►►

Implementation Strategy

The Firm must submit to FinCEN an initial, and thereafter annual, notice, which can be completed online at FinCEN's Web site (www.fincen.gov) prior to sharing information. Prior to sharing information, the Firm must take reasonable steps to ensure that the other firm with which it intends to share this information has submitted the requisite notice to FinCEN. This can be done by confirming that the other firm appears on a list that FinCEN will make available on a periodic basis to firms that have filed a notice with them, or by confirming directly with the other firm that the requisite notice has been filed. The Firm can obtain a copy of the other firm's notice, or by other reasonable means, including accepting the representations of the other firm that a notice was filed after the most recent list has been distributed by FinCEN.

However, in the event that the Firm receives information requests, the information received by the Firm under a sharing agreement cannot be used for any other purpose other than identifying and where appropriate, reporting on money laundering or terrorist activities, determining whether to establish or maintain an account or engage in a transaction, or assisting the financial institution in complying with any requirement of the section.

10.16 Information Requests under Section 314(a) of the USA PATRIOT Act

Section 314(a) of the USA PATRIOT Act of 2001 requires the Secretary of the Treasury to adopt regulations to encourage regulatory authorities and law enforcement authorities to share with financial institutions information regarding individuals, entities, and organizations engaged in or reasonably suspected, based on credible evidence, of engaging in terrorist acts or money laundering activities.

FinCEN issued a proposed rule on March 5, 2002 and the final rule on September 26, 2002 (67 Fed. Reg. 60,579).

FinCEN's regulations under Section 314(a) enables federal law enforcement agencies, through FinCEN, to reach out to 41,468 points of contact at more than 20,000 financial institutions to locate accounts and transactions of persons that may be involved in terrorism or money laundering. FinCEN receives requests from federal law enforcement and upon review, transmits requests to designated contacts within financial institutions across the country. The requests contain subject and business names, addresses, and other identifying data.

Pursuant to section 314(a) of the USA PATRIOT Act, the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) developed and implemented an electronic system for law enforcement to request information about suspected terrorists and money launderers from financial institutions. Every two weeks, FinCEN distributes a 314(a) subject list by e-mail to financial institution points of contact (POCs) for this purpose.

FinCEN introduced a new Web-based section 314(a) delivery and reporting system. In the new system, FinCEN will not send attachments through e-mails. Instead, FinCEN will e-mail a secure Web page location to all 314(a) POCs. POCs are responsible for accessing the Web page (URL) on the Internet where the 314(a) subject lists are located, download the files in various formats for searching (i.e., tab delineated, MS Word, MS Excel, etc.), and use the Internet site to return positive and inconclusive hits to FinCEN.

Therefore, beginning on March 1, 2005, FinCEN will no longer distribute the 314(a) subject lists by e-mail attachments. Instead, the 314(a) subject lists will be posted to the secure web site every two weeks, and financial institutions will be required to access the Web site to obtain the lists and conduct the searches within required timeframes. ►►

Implementation Strategy

Within five days of receipt of each email notification, the designated AMLCO or his designee will access the secure Web page (https://www.fincen.gov/314a/) for updated 314(a) information and download all relevant files in an acceptable format to facilitate searching capabilities. During review, the AMLCO or his designee reviews and reconciles with the Firm's existing records for data matches, including accounts maintained by the named subject during the preceding 12 months and transactions conducted within the last six months. In the event of a positive match, the Firm's AMLCO will access the Internet site and report any such findings and promptly investigate and document each case and determine the appropriate action for a prompt resolution within forty-eight hours of any positive match. Upon receipt of each 314(a) notification, the AMLCO will maintain
documentation
as evidence of review.

10.17 Emergency Notification to the Government by Telephone

In accordance with NTM 02-21, broker/dealers should identify contact persons and have procedures in place for providing information to and handling requests from enforcement authorities about the firms' AML efforts, as well as customers engaged in possible money laundering. This information must be provided to the appropriate agency and made available at a specified location when requested. Firms should establish procedures to provide such information *not later than seven days* after receiving a written enforcement agency request. ►►

Implementation Strategy

When conducting due diligence or opening an account, we will immediately call Federal law enforcement when necessary, and especially in these emergencies: a legal or beneficial account holder or person with whom the account holder is engaged in a transaction is listed on or located in a country or region listed on the OFAC list, an account is held by an entity that is owned or controlled by a person or entity listed on the OFAC list, a customer tries to use bribery, coercion, or similar means to open an account or carry out a suspicious activity, we have reason to believe the customer is trying to move illicit cash out of the government's reach, or we have reason to believe the customer is about to use the funds to further an act of terrorism. We will first call the OFAC Hotline at 1-800-540-6322. The other contact numbers we will use are: Financial Institutions Hotline (1-866-556-3974), local U.S. Attorney's Office, local FBI Office, and local SEC Office.

10.18 SAR-SF Maintenance and Confidentiality

The Firm will hold all SAR-SF Reports and any supporting documentation strictly confidential. The Firm will not inform anyone outside of a law enforcement or regulatory agency or securities regulator about a SAR-SF. Additionally, the Firm will refuse any subpoena requests for SAR-SFs or SAR-SF information and immediately tell FinCEN of any such subpoena that may be received.

The Financial Crimes Enforcement Network (FinCEN) regulations regarding the confidentiality of suspicious activity reports (SARs) require a broker-dealer to make SARs and supporting documentation available to any self-regulatory organization (SRO) that examines the broker-dealer for compliance with the requirements of 31 CFR 1023.320 (the SAR Rule), upon the request of the SEC. On January 26, 2012, the SEC issued a letter to FINRA authorizing FINRA staff to ask for SARs and SAR information from member firms in certain circumstances. On the same date, SEC staff also issued a letter to chief executive officers of all SEC-registered FINRA member firms requesting that they make SARs and supporting documentation available to FINRA.

The SEC's request applies to all FINRA member firms and applies to requests in connection with FINRA's:

- examinations;
- investigations; and
- risk assessment efforts within its examination program.

FINRA staff may request SARs and SAR information, or question firm staff, about SAR related activity from any time frame within the examination or investigation review period, including any time prior to the SEC issuance of the letter. (Ref. Regulatory Notice 12-08; February 2012) ►►

Implementation Strategy

The Firm's designated AML Compliance Officer will handle all subpoenas or other requests for SAR-SFs. In the event the Firm maintains a correspondent relationship with a designated clearing firm, the Firm may share information with its designated clearing firm about suspicious transactions in order to determine when a SAR-SF should be filed. Additionally, the Firm may share with the clearing firm a copy of the filed SAR-SF – unless it would be inappropriate to do so under the circumstances, such as where we file a SAR-SF concerning the clearing firm or its employees. The Firm will segregate SAR-SF filings and copies of supporting documentation in a secured location separate from other firm books and records to avoid disclosing SAR-SF filings. Additionally, the Firm may share SARs and SAR Information upon request from FINRA in connection with

FINRA examinations, investigations and risk assessment efforts within its examination program.

Confidential Reporting of AML Non-Compliance

Employees will report any violations of the Firm's AML compliance program to the AML Compliance Officer, unless the violations implicate the Compliance Officer, in which case the employee shall report to the President or other authorized executive officer of the Firm. Such reports will be confidential, and the employee will suffer no retaliation for making them.

10.19 Special Measures against Specified Banks Pursuant to 311 of the USA PATRIOT ACT

The Financial Crimes Enforcement Network (FinCEN) has issued a final rule imposing a special measure, which becomes effective August 14, 2006, against the Latvian bank VEF Banka and its subsidiaries. This measure is comparable to that imposed against the Commercial Bank of Syria and its subsidiaries, including Syrian Lebanese Commercial Bank, which became effective April 14, 2006.

Effective April 18, 2007, Financial Crimes Enforcement Network (FinCEN) issued a final rule imposing a special measure against Banco Delta Asia SARL, including its subsidiaries Delta Asia Credit Limited and Delta Asia Insurance Limited (Banco Delta Asia or bank). Banco Delta Asia is a commercial bank in Macau, Special Administrative Region, China. This measure is comparable to that imposed against the Latvian bank VEF Banka and its subsidiaries, including Veiksmes lizings (NTM 07-17; Effective April 18, 2007)

The special measures have been imposed in response to findings that these entities and their subsidiaries (the "Specified Banks") are financial institutions of primary money laundering concern. Under the special measures, covered financial institutions, which includes broker-dealers, are subject to the following two primary requirements with respect to the Specified Banks:

- **Prohibition of the Direct Use of Correspondent Accounts by the Specified Banks**. Covered financial institutions are prohibited from opening or maintaining a correspondent account in the United States for, or on behalf of, the Specified Banks. This prohibition requires all covered financial institutions to review their account records to ensure that they maintain no accounts directly for, or on behalf of, the Specified Banks to the extent that such indirect use can be determined from transactional records maintained by the covered financial institution in the normal course of business. A covered financial institution must take a risk-based approach when deciding what, if any, additional due diligence measures it should adopt to guard against the indirect use of correspondent accounts by the Specified Banks, based on risk factors such as the type of services offered by, and geographic locations of, its correspondents**.** Unlike the duties imposed under the one-time notification requirement, covered financial institutions have an ongoing obligation to take reasonable steps to identify all correspondent account services they may directly or indirectly provide to the Specified Banks (NTM 070-17; Effective April 18, 2007)

- **Due Diligence to Prevent Indirect Use.** As a corollary to the prohibition on the opening or maintaining of correspondent accounts directly for the Specified Banks, each covered financial institution is required to apply due diligence to its correspondent accounts that is reasonably designed to guard against their indirect use by the Specified Banks. At a minimum, such due diligence must include two elements: (1) *Notification to Correspondent Accountholders*- A covered financial institution must notify its correspondent accountholders that the account may not be used to provide the Specified Banks with access to the covered financial institution; (2) *Identification of Indirect Use***-** A covered financial institution must take

reasonable steps in order to identify any indirect use of its correspondent accounts by the Specified Banks, to the extent that such indirect use can be determined from transactional records maintained by the covered financial institution in the normal course of business. A covered financial institution must take a risk-based approach when deciding what, if any, additional due diligence measures it should adopt to guard against the indirect use of correspondent accounts by the Specified Banks, based on risk factors such as the type of services offered by, and geographic locations of, its correspondents. (Ref. NTM 06-41; Effective Aug. 14, 2006) ►►

Implementation Strategy

The Firm will not open or maintain any correspondent accounts for or on behalf of the Specified Banks as referenced above. The AMLCO will review the Firm's account records to ensure that the Firm is refraining from opening and/or maintaining any accounts directly for, or on behalf of, the Specified Banks.

10.20 Burma Sanctions

Burma Sanctions

On July 11, 2012, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") relaxed certain economic sanctions against Burma (Myanmar). As a result of this change, it is now permissible to:

- Provide brokerage services to customers located in Burma (whether temporarily or permanently).
- Process funds transfers to and from Burma; and
- Trade securities in non-Burmese companies that derive most or all of their revenue from Burma.

It remains prohibited to have any dealings with any Burmese individuals or entities on OFAC's List of Specially Designated Nationals and Blocked Persons ("SDN List").

In addition, investments or transactions involving the Burmese Ministry of Defense (including the Office of Procurement), any state or non-state armed services in Burma, or any entity in which the Ministry of Defense or the armed services in Burma owns a 50 percent or greater interest are prohibited. ►►

Implementation Strategy

The Firm will carefully monitor its brokerage services (e.g. fund transfers, securities trading activity) to customers located in Burma. In an effort to monitor for such accounts, the designated supervisor will review new account activity to effectively screen for any customer accounts located in Burma to check for any investments or transactions involving the Burmese Ministry of Defense (including the Office of Procurement), any state or non-state armed services in Burma, or any entity in which the Ministry of Defense or the armed services in Burma owns a 50 percent or greater interest which are strictly prohibited.

10.21 AML Act & AML/CFT Priorities

The Financial Crimes Enforcement Network (FinCEN) has issued the first government-wide priorities for anti-money laundering and countering the financing of terrorism policy, which was mandated by the Anti-Money Laundering Act of 2020 (AML Act). FinCEN also issued a statement to provide covered non-bank financial institutions (NBFIs), including broker-dealers, with guidance on how to approach the AML/CFT Priorities.

AML/CFT Priorities

The AML Act became law on January 1, 2021, and, among other amendments to the Bank Secrecy Act (BSA), requires FinCEN to issue the AML/CFT Priorities and update them at least once every four years. On June 30, 2021, FinCEN, the bureau of the Department of the Treasury responsible for administering the BSA and its implementing regulations, issued its first government-wide AML/CFT Priorities. The AML/CFT Priorities are intended to assist covered financial institutions, including broker-dealers, in their efforts to meet their obligations under laws and regulations designed to combat money laundering and counter terrorist financing.

The AML/CFT Priorities focus on threats to the U.S. financial system and national security and reflect longstanding and continuing AML/CFT concerns previously identified by FinCEN and other U.S. government departments and agencies. They include predicate crimes to money laundering that generate illicit proceeds that illicit actors may launder through the financial system.

FinCEN set forth eight priorities: (1) corruption; (2) cybercrime, including relevant cybersecurity and virtual currency considerations; (3) foreign and domestic terrorist financing; (4) fraud (including securities and investment fraud and internet-enabled fraud); (5) transnational criminal organization activity; (6) drug trafficking organization activity; (7) human trafficking and human smuggling; and (8) proliferation financing. FinCEN provides details about each of the individual priorities and includes references to prior FinCEN advisories and guidance documents that identify related typologies and red flags that may help broker-dealers comply with their BSA obligations.

The BSA, as amended by the AML Act, provides that the “review by a financial institution” of the AML/CFT Priorities and “the incorporation of those priorities, as appropriate” into the risk-based AML compliance programs established by the financial institution “shall be included as a measure on which a financial institution is supervised and examined for compliance.”

Although the issuance of the AML/CFT Priorities does not trigger an immediate change in the BSA requirements or supervisory expectations for member firms, member firms are encouraged to evaluate how they will incorporate and document the AML/CFT Priorities, as appropriate, into their risk-based AML programs. Member firms that are beginning to evaluate how they will do so may wish to begin considering potential updates to the red flags that they have incorporated into their risk-based AML compliance programs in light of the risks presented by factors such as their business activities, size, the geographic locations in which they operate, the types of accounts they maintain, and the types of transactions in which they and their customers engage.

Firms should also consider any potential technological changes that may be appropriate in order to incorporate the AML/CFT Priorities into their risk-based AML compliance programs, including changes to the technology that they use to monitor and investigate suspicious activity.

Corruption

Corrupt actors and their financial facilitators may seek to take advantage of vulnerabilities in the U.S. financial system to launder their assets and obscure the proceeds of crime. Misappropriation of public assets, bribery, and other forms of corruption affects individuals and entities across the world, threatens the national security of the United States and the global financial system, degrades the rule of law, perpetuates conflict, and deprives innocent civilians of fundamental human rights.

FinCEN has issued advisories on human rights abuses enabled by corrupt senior foreign political figures and their financial facilitators with respect to Nicaragua, South Sudan, and Venezuela. These advisories, while focused on specific foreign jurisdictions, can help covered institutions comply with their BSA obligations by identifying typologies and red flags, but the jurisdictions noted in those advisories are not the only ones at risk of corruption.

Cybercrime, including Relevant Cybersecurity and Virtual Currency Considerations

Cybercrime is broadly defined as any illegal activity that involves a computer, another digital device, or a computer network. Cybercrime includes common cybersecurity threats like social engineering, software vulnerability exploits, and network attacks. Cybercrime is a significant illicit finance threat: the size, reach, speed, and accessibility of the U.S. financial system make covered institutions attractive targets to criminals, including terrorists and state actors. These actors target covered institutions' websites, systems, and employees to steal customer and commercial credentials and proprietary information, defraud covered institutions and their customers, and disrupt business functions. Treasury is particularly concerned about cyber-enabled financial crime, ransomware attacks, and the misuse of virtual assets that exploits and undermines their innovative potential, including through laundering of illicit proceeds.

FinCEN has issued advisories with respect to ransomware and COVID-19-related cybercrime, including cyber-enabled financial crime, to alert covered institutions to predominant trends, typologies, and potential indicators. Regarding the COVID-19 pandemic, FinCEN advised covered institutions that criminals increasingly exploited the pandemic through phishing campaigns and the compromise of remote applications to facilitate extortion, business email compromise (BEC), and other fraudulent schemes, especially against financial and health care systems. Ill-gotten gains from these illicit activities often are laundered through a variety of methods, including rapid transfers through accounts controlled by the cyber actors or money mules. Covered institutions are uniquely positioned to observe the suspicious activity that results from cybercrime, including cyber-enabled financial crime. FinCEN recently issued a fact sheet to encourage covered institutions to share such information with one another under a safe harbor provision of the BSA that offers protections from civil liability, in order to better identify and report potential money laundering or terrorist financing.

Terrorist Financing

Covered institutions are reminded of existing obligations to identify and file SARs on potential terrorist financing transactions, as appropriate, and follow applicable requirements for reporting violations requiring immediate attention. Terrorist financing includes lone actors using small amounts of money to self-fund attacks, as well as more complex schemes and networks that may be embedded within existing money laundering methods used to support logistical networks, operatives, and the procurement of material.

As a countermeasure to these potential risks, covered institutions must comply with required sanctions programs and, as part of their risk-based AML programs, also should be aware of terrorists and terrorist organizations that are included on sanctions lists issued by the U.S. government.

Fraud

As previously noted in Treasury's National Money Laundering Risk Assessments, the crimes that generate the bulk of illicit proceeds in the United States are fraud, drug trafficking, human smuggling, human trafficking, organized crime, and corruption. Among those, fraud—such as bank, consumer, health care, securities and investment, and tax fraud—is believed to generate the largest share of illicit proceeds in the United States. Increasingly, fraud schemes are internet-

enabled, such as romance scams, synthetic identity fraud, and other forms of identity theft. Proceeds from fraudulent activities may be laundered through a variety of methods, including transfers through accounts of offshore legal entities, accounts controlled by cyber actors, and money mules.

FinCEN has issued several fraud-related advisories, in particular with respect to BEC, email account compromise, and COVID-19. Also of concern are foreign intelligence entities and their proxies, which employ illicit financial practices to fund influence campaigns and facilitate a range of espionage activity by establishing front companies, and conducting targeted investments to gain access to sensitive U.S. individuals, information, technology and intellectual property.

Transnational Criminal Organization Activity

Transnational criminal organizations (TCOs) operating in the United States, including drug trafficking organizations (DTOs), are priority threats due to the crime-terror nexus and TCOs' engagement in a wide range of illicit activities. Treasury has noted that a number of TCOs operate in the United States, and Mexican and Russian TCOs operating in the United States remain priority threats. In addition, certain Africa- and Asia-based TCOs become more significant each year as TCOs worldwide continue to employ a variety of money laundering methods to avoid detection. Increasingly, these organizations turn to professional money laundering networks that receive a fee or commission for their laundering services, and often use their specialized expertise to launder proceeds generated by others, regardless of the predicate criminal activity.

Drug Trafficking Organization Activity

DTOs rely more on professional money laundering networks in Asia (primarily China) that facilitate exchanges of Chinese and U.S. currency or serve as money brokers in trade-based money laundering (TBML) schemes. There has been a substantial increase in complex schemes to launder proceeds from the sale of narcotics by facilitating the exchange of cash proceeds from Mexican DTOs to Chinese citizens residing in the United States, including the use of front companies or couriers to deposit cash derived from the sale of narcotics into the banking system. These schemes allow DTOs to repatriate proceeds to Mexico and sidestep Chinese capital flight restrictions.

Human Trafficking and Human Smuggling

Financial activity from human trafficking and human smuggling activities can intersect with the formal financial system at any point during the trafficking or smuggling process. FinCEN, in collaboration with law enforcement agencies, nonprofit organizations, and members of the financial industry, issued two advisories identifying financial and behavioral red flags of human trafficking, as well as financial red flags associated with human smuggling. Human trafficking and human smuggling networks use a variety of mechanisms to move illicit proceeds, ranging from cash smuggling by individual victims to sophisticated cash smuggling operations through professional money laundering networks and criminal organizations.

Proliferation Financing

The principal threat of proliferation financing arises from proliferation support networks. These networks of individuals and entities, such as trade brokers and front companies, seek to exploit the U.S. financial system to move funds that will be used either: (1) to acquire weapons of mass destruction or delivery systems or their components; or (2) in the furtherance or development of state-sponsored weapons programs, including the evasion of United Nations or U.S. sanctions.

Actors engaged in the proliferation of weapons of mass destruction have developed sophisticated and diverse strategies to finance their programs. Covered institutions remain vulnerable to malign actors seeking to generate revenues and transfer funds in support of illicit conduct through gatekeepers, front or shell companies, exchange houses, or the illicit exploitation of international trade. Covered institutions are encouraged to consult FinCEN's advisories with respect to jurisdictions with AML/CFT and counter-proliferation deficiencies for additional information regarding the risk of proliferation finance. As a counter-measure to these potential risks, covered institutions must comply with sanctions programs and, as part of a risk-based AML program, should also be aware of economic and trade sanctions issued by the federal government, such as OFAC, the Department of Commerce's Bureau of Industry and Security, and the Department of State's Bureau of International Security and Nonproliferation. (Ref. Regulatory Notice 21-36; October 8, 2021)

Implementation Strategy

In an effort to combat money laundering and counter terrorist financing, the Firm's designated supervisor will review the eight major areas under the AML/CFT Priorities that include (1) corruption; (2) cybercrime, including relevant cybersecurity and virtual currency considerations; (3) foreign and domestic terrorist financing; (4) fraud (including securities and investment fraud and internet-enabled fraud); (5) transnational criminal organization activity; (6) drug trafficking organization activity; (7) human trafficking and human smuggling; and (8) proliferation financing, to evaluate how the Firm will incorporate and document the AML/CFT Priorities, as appropriate, into its risk-based AML Program. Such updates may include periodic reviews if its current AML Program and possible updates to red flags in light of the risks presented by factors such as the Firm's business activities, geographical location(s) in which it operates, the type of accounts and maintained and the types of transactions in which the Firm and its customers engage.